HAAGA-HELIA
ammattikorkeakoulu

Pk-yrityksen tietoturva

Satu Leino

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2013

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

30.6.2013

Tietojenkäsittelyn koulutusohjelma

Tekijä Satu Leino	**Ryhmätunnus tai aloitusvuosi** 2008
Opinnäytetyön nimi Pk-yrityksen tietoturva	**Sivu- ja liitesivumäärä** 48+3
Ohjaaja Titta Ahlberg	

Tämän opinnäytetyön tavoitteena oli tutkia pk-yritysten tietoturvaa vuonna 2013. Opinnäytetyö toteutettiin perehtymällä aihealueen kirjallisuuteen ja työn empiirisessä osassa selvitettiin pk-yritysten tietoturvan tasoa kyselytutkimuksen avulla. Opinnäytetyö rajattiin koskemaan hallinnollista tietoturvaa, henkilöstöturvallisuutta ja tietoturvan teknistä toteuttamista.

Opinnäytetyöhön liittyvän tutkimuksen tavoitteena oli selvittää, mikä on tämän hetkinen tietoturvan taso suomalaisissa pk-yrityksissä. Tutkimuksen avulla selvitettiin pk-yritysten käytössä olevia tietoturvaratkaisuja, henkilöstöön ja liiketoimintaan liittyvien tietoturva-asioiden hoitoa sekä selvitettiin salasanojen käyttötottumuksia.

Tutkimus toteutettiin kvantitatiivisena tutkimustyönä ja aineiston keräystavaksi valittiin kysely. Verkkokysely toteutettiin toukokuussa 2013 ja siihen vastasi 65 pk-yrityksen edustajaa.

Tutkimuksen tuloksena voidaan todeta että tekninen tietoturvallisuus on hoidettu pk-yrityksissä keskimäärin hyvin, mutta tietoturvan hallinnollisessa puolessa on yhä parantamisen varaa.

Asiasanat
tietoturvallisuus, tietosuoja, pienet ja keskisuuret yritykset

HAAGA-HELIA
University of Applied Sciences

Abstract

30.6.2013

Degree Programme in Information Technology

Author Satu Leino	**Group or year of entry** 2008
The title of thesis Information Security in Small and Medium Sized Enterprises	**Number of report pages and attachment pages** 48 + 3
Advisor Titta Ahlberg	

The objective of this thesis was to examine the current state of information security in small and medium sized enterprises (SMEs) in Finland. The study investigated information security solutions, personnel related security issues and business related security issues and password habits.

The study included a theory section and an empirical section. The information for the theoretical background was gathered to explain the main topics and concepts related to the subject and the empirical part of the thesis was executed by conducting an online survey in May 2013 and 65 SME representatives responded to it. The study was based on quantitative methods.

The thesis indicated that the technical aspects of information security were implemented well in SMEs, but administrative security matters still have some space for improvement.

Key words
information security, data protection, small and medium sized enterprises (SMEs)

Sisällys

1 Johdanto

Tämän päivän yritysmaailmassa monet toiminnot ovat voimakkaasti sidoksissa tietotekniikkaan. Tieto on yritykselle tärkeää pääomaa, ja sen turvaamisesta on tullut yritysten toiminnan edellytys. Toimintojen ja palveluiden sähköistyessä, tietoturvallisuudesta huolehtiminen on korostunut entisestään. Asianmukainen tietoturvaturvallisuudesta huolehtiminen on tärkeää paitsi yrityksen oman toiminnan, myös erityisesti asiakkaiden ja muiden sidosryhmien kannalta.

Tällä opinnäytetyöllä ei ole toimeksiantajaa, vaan idea aiheen tutkimiseen lähti omasta kiinnostuksestani tietoturvaan liittyviä asioita kohtaan. Tutkimuksen kohderyhmäksi valitsin pk-yritykset, koska koin pienempien yritysten hyötyvän tutkimuksesta eniten.

1.1 Tavoitteet, tutkimusongelma ja rajaus

Tämän opinnäytetyön tavoitteena on kartoittaa tärkeimpiä pk-yrityksiä koskevia tietoturvakysymyksiä ja löytää niihin ratkaisuja. Tutkimus pyrkii vastaamaan kysymyksiin: ”Mitkä ovat tärkeimmät pk-yrityksiä koskevat tietoturvakysymykset?” ja ”Mikä on tämänhetkinen tietoturvan taso pk-yrityksissä?”. Opinnäytetyöhön liittyvän kyselytutkimuksen avulla selvitetään tietoturvan tasoa kohdeyrityksissä. Kyselyssä selvitetään niin teknisen tietoturvan kuin henkilöstöön ja liiketoimintaan liittyviä tietoturvakysymyksiä pk-yrityksissä. Tämän lisäksi kartoitetaan salasanojen käyttötottumuksia.

Pk-yrityksen tietoturva on erittäin laaja aihealue, josta oli rajattava pienempi osa-alue opinnäytetyössä tehtävää tarkastelua varten. Tässä työssä päädyttiin tutkimaan pk-yrityksen hallinnollista tietoturvaa erityisesti liiketoiminnan ja henkilöstön kannalta. Opinnäytetyössä tutkitaan osittain myös tietoturvan teknistä toteuttamista. Työ rajattiin koskemaan pienten ja keskisuurten yrityksen tietoturvaa.

1.2 Tutkimuksen rakenne

Opinnäytetyö jakautuu seitsemään lukuun. Luvuissa 2 – 4 muodostetaan teoreettinen viitekehys aiheesta. Teoriatausta keskittyy tietoturvan peruskäsitteiden määrittelyyn ja tietoturvan merkityksen selvittämiseen liiketoiminnan kannalta. Tämän jälkeen teo-

riataustassa esitellään hallinnollisen tietoturvan erityispiirteitä ja lopuksi keskitytään tietoturvan tekniseen toteuttamiseen. Luvussa 5 käydään läpi tutkimuksen tausta ja esitellään kaksi aiheesta aiemmin tehtyä tutkimusta. Luvussa esitellään myös tutkimusongelma, tutkimuksen kohderyhmä, tutkimusmenetelmät ja tutkimuksen toteutus. Tutkimuksen tuottamat tulokset esitellään luvussa 6. Lisäksi saatuja tuloksia verrataan aiempiin aiheesta tehtyihin tutkimuksiin. Luvussa 7 esitellään tulosten johtopäätökset ja suositukset jatkoa varten esitellään luvussa sekä arvioidaan omaa oppimista opinnäytetyöprosessin aikana.

2 Tietoturva

Yritysten liiketoimintaympäristö on muuttunut ja liiketoiminta on tullut yhä riippuvaisemmaksi tiedosta ja tietojärjestelmistä. Tämän kehityksen myötä myös yrityksen tietoturvallisuudesta huolehtiminen on kasvattanut merkitystään. Tässä luvussa käydään läpi tietoturvan määritelmä, keskeiset käsitteet ja tietoturvan osa-alueet sekä kerrotaan tietoturvan ja tietosuojan merkityksestä liiketoiminnassa.

2.1 Tietoturvan määritelmä

Klassinen tietoturvan määritelmä koostuu kolmesta osatekijästä, jotka ovat luottamuksellisuus, käytettävyys ja eheys. Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain tietoon oikeutettujen henkilöiden käytettävissä. Käytettävyys merkitsee sitä, että tiedot ovat saatavissa oikeassa muodossa ja riittävän nopeasti. Eheys puolestaan tarkoittaa sitä, että tietojärjestelmän tiedot pitävät paikkaansa eivätkä ne sisällä virheitä. (Hakala, Vainio & Vuorinen 2006, 4.)

Tietoturvallisuudella tarkoitetaan tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista ja niihin kohdistuvien riskien hallitsemista kaikissa olosuhteissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuuden tavoitteena on tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen erilaisten vikojen, uhkien ja vahinkojen osalta. (Andreasson & Koivisto 2013b, 29.)

Luottamuksellisuuden ylläpitoon pyritään suojaamalla tietojärjestelmät käyttäjätunnuksin ja salasanoin. Arkaluontoiset tai erityisen arvokkaat tiedot voidaan suojata salaamalla ne erilaisin salakirjoitusmenetelmin. Käytettävyyttä ylläpidetään huolehtimalla siitä että tietojärjestelmien laitteet ovat riittävän tehokkaita ja että käytettävät ohjelmistot soveltuvat käyttötarkoitukseensa mahdollisimman hyvin. Eheyteen pyritään pääasiassa ohjelmistoteknisin keinoin, ohjelmoimalla järjestelmiin erilaisia tarkistuksia ja käyttämällä virheentunnistusmekanismeja. (Hakala ym. 2006, 4-5.)

Klassinen määritelmä sisältää olennaisimmat asiat, joista on huolehdittava ennen muita tietoturvallisuuden osatekijöitä. Klassista määritelmää pidetään kuitenkin riittämättö-

mänä, koska se ei huomioi tarpeeksi tiedon tuottajan tai omistajan identiteettiä, eikä laitteistojen tai tietojärjestelmien ja tietoliikennejärjestelmien arvoa. Klassista määritelmää onkin laajennettu sisältämään käsitteet kiistämättömyys ja pääsynvalvonta. (Hakala ym. 2006, 5.)

Kiistämättömyydellä tarkoitetaan tietojärjestelmän kykyä tunnistaa ja tallentaa luotettavasti järjestelmää käyttävän henkilön tiedot. Kiistämättömyyteen pyritään käyttämällä salausmenetelmiin liittyviä tunnistusmekanismeja tai biometrisiä tunnisteita. Pääsynvalvonta käsittää ne menetelmät, joilla rajoitetaan tietojenkäsittelyjärjestelmien käyttöä. Varsinaisiin tietoihin pääsyn rajoittaminen kuuluu luottamuksellisuuden ylläpitoon. Pääsynvalvontaan on jouduttu kiinnittämään entistä enemmän huomiota langattomien verkkojen yleistettyä. (Hakala ym. 2006, 5.)

Tietoturvallisuustyön päämääränä on turvata liiketoiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tiedon tuhoutuminen tai vääristyminen sekä minimoida vahingot. Tietoturvallisuuteen tulisi kiinnittää huomiota erityisesti ulkoistettaessa tietojenkäsittelyyn liittyviä toimintoja, otettaessa käyttöön uusia toimintamalleja tai tehtäessä hankintoja. (Andreasson & Koivisto 2013b, 29.)

2.2 Tietoturvan osa-alueet

Tietoturvallisuus on laaja kokonaisuus, joka voidaan jakaa eri osa-alueisiin usealla eri tavalla. Perinteinen tapa on jakaa tietoturva kahdeksaan alueeseen, jotka ovat:

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus.

Jotkut tahot ovat sitä mieltä, että ulkoistaminen muodostaa oman osa-alueensa tietoturvallisuuteen kahdeksan edellämainitun lisäksi. (Andreasson & Koivisto 2013b, 52.)

Tietoturvallisuuteen liittyy läheisesti myös tietosuoja. Molemmissa on kyse tietojen suojaamisesta, mutta tietojen sisältö ja suojaamisen tarkoitus ovat erilaiset. Tietoturvassa suojataan itse tietoja ja tietojärjestelmiä. Samalla pyritään varmistamaan järjestelmien toiminta kaikissa olosuhteissa sekä käytön turvallisuus tietoturvan periaatteiden mukaisesti. Tietosuojan kohteena ovat ihmisten henkilötiedot. Tietosuojalla pyritään takaamaan henkilöille oikeus yksityisyyteen sekä estämään tietojen tarpeeton tai epäasiallinen käyttö. (Järvinen 2012,12.) Tietosuojalla on perinteisesti tarkoitettu henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten henkilöiden yksityydensuojan ja oikeusturvan varmistamiseksi. Tietosuojan tarkoituksena on ohjata rekisterinpitäjiä hyvään henkilötietojen käsittelytapaan ja turvata tiedon kohteen yksityisyyttä, etuja ja oikeuksia. (Andreasson, Koivisto & Ylipartanen 2013a, 14.)

2.3 Tietoturvan merkitys liiketoiminnassa

Tiedot ja tietoturvallisuus ovat nykypäivän yhteiskunnassa ehdottomia edellytyksiä yrityksen toiminnalle. Yrityksen toiminta voi pysähtyä täysin jos toimintaympäristön tarvitsemat tiedot, tietojärjestelmät ja yhteydet eivät ole saatavilla. Tietojen tulee lisäksi olla oikeita ja luotettavia. Asianmukaisella tietojen suojauksella turvataan yrityksen toimintaympäristöä, yhteiskuntaa sekä asiakkaiden ja yhteistyökumppaneiden tietoja. Tietojen luvaton päätyminen ulkopuolisille voi vaarantaa toimintaympäristön turvallisuuden ja palveluiden jatkuvuuden. Yrityksen tulee omaan toimintaansa liittyvien tietojen lisäksi huolehtia myös sidosryhmiensä ja erityisesti asiakkaidensa tiedoista. (Valtiovarainministeriö 2011, 13.)

Tietoturva ja tietosuoja ovat Suomen lainsäädännön mukaan osa yrityksen päivittäistä toimintaa ja koskevat organisaation koko toimintaa ja henkilöstöä. Yhteiskunta ja yritysmaailma ovat entistä riippuvaisempia tietojärjestelmistä ja niiden toimintavarmuudesta. Tietoturvan tärkeyttä lisäävät tietojärjestelmien etäkäytön ja mobiilikäytön lisääntyminen sekä uudet palvelumenetelmät, muun muassa pilvipalvelut, joita käytettäessä

tietojen sijainti hämärtyy. Yhteiskunta on nykyään pitkälti riippuvainen tietojen käsittelystä ja verkottuneessa ympäristössä yritykset ovat vastuussa itsensä lisäksi myös muiden tietoturvallisuudesta. Tietoturvallisuus on osa organisaation toiminnan laatua ja riskienhallintaa. (Andreasson ym. 2013a, 30-32.)

Tietoturvallisuuden ensisijaisena tarkoituksena on turvata yrityksen vastuulla olevien palveluiden jatkuvuus kaikissa olosuhteissa. Tietojen, järjestelmien ja palveluiden on pysyttävä toiminnassa ja niiden on oltava saatavilla silloin kuin niitä tarvitaan. Tietoturvan ja tietosuojan toteuttamissa tulisi tarvittaessa käyttää ulkopuolisten asiantuntijoiden apua jos omasta yrityksestä ei löydy tarvittavaa osaamista. (Andreasson ym. 2013a, 32-33.)

Hyvin toteutettuna tietoturvallisuus rakennetaan osaksi yrityskulttuuria, jolloin koko henkilöstö ymmärtää tietoturvan merkityksen ja työskentelee sen saavuttamiseksi ja ylläpitämiseksi. Tietoturvallisuus pitää sisällään teknisiä ja hallinnollisia toimenpiteitä, jotka tulee suunnitella huolella lainsäädännön vaatimukset huomioon ottaen ja joiden vaikutuksia tulee seurata toiminnan kehittämiseksi. Hyvän tietoturvallisuustason saavuttaminen ja ylläpitäminen vaatii yritykseltä määrätietoista toimintaa ja johtamista. Tietoturvaa ei tulisi nähdä välttämättömänä pahana, jolla kiusataan työntekijöitä vaan se pitäisi nähdä yrityksen kilpailuetuna. Tämä tietenkin edellyttää että tietoturva on hoidettu asianmukaisesti liiketoiminnan vaatimusten edellyttämällä tavalla. (Laaksonen, Nevasalo & Tomula 2006, 17-18.)

Petri Puhakaisen vuonna 2006 tarkastetun väitöskirjan ”A design theory for information security awareness” mukaan yritykset keskittyivät yhä liikaa teknisiin menettelytapoihin ja turvatoimiin, joiden hyöty menetetään jos henkilöstö ei ole tietoinen niiden merkityksestä. Hallinnollisilla toimilla ja henkilöstön koulutuksella voidaan väitöskirjan mukaan saada aikaan merkittäviä tuloksia tietoturvallisuuden kehittämisessä. (Puhakainen 2006.)

Tietotekniikanliitto ry:n vuonna 2006 teettämän Pk-tietoturvatutkimuksen mukaan pk-yritykset keskittyivät suojaamaan tietojärjestelmänsä pääasiassa teknisin keinoin, vaikka työntekijöiden tahattomien virheiden ja tietämättömyyden koetaan uhkaavan tietotur-

vallisuutta eniten. Tutkimuksen mukaan yritykset näkevät merkittävämpänä yksittäisenä tietoturvaongelmana työntekijät, joiden taidot ja osaaminen eivät vastaa vaatimuksia. (Tietotekniikan liitto ry 2007.)

Paavo Porvarin vuonna 2012 tarkastetun väitöskirjan ”Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöstön toiminnassa” mukaan teknisillä toimilla voidaan toteuttaa vain kolmasosa tietoturvallisuudesta ja yritysten tietoturvassa on puutteita kaikilla osa-alueilla. Porvarin mukaan keskittyminen teknisiin ratkaisuihin johtuu useasta eri syystä. Pk-yrityksissä ollaan vielä osittain siinä tietoturvallisuuden hallinnan vaiheessa, jossa tietoturvallisuus jätettiin asiantuntijoiden tehtäväksi. Resursseja on vähän ja asiantuntemus riskeistä ja turvakäytännöistä on puutteellista. (Porvari 2012, 212.)

Myös Porvarin väitöskirjassa todetaan että tietoturvallisuudesta huolehtiminen on yritysjohton vastuulla. Tietoturvariskit ovat liiketoimintariskejä ja tästä johtuen niitä tulee käsitellä yrityksen ylimmässä johdossa. Porvarin väitöskirjan mukaan tätä ei ole pk-yrityksissä tiedostettu ja yrityksissä tulisikin päästä tavoitteelliseen ja jatkuvaan tietoturvatoimintaan. Tämän lisäksi on erittäin tärkeää saada koko henkilökunta motivoiduksi tietoturvallisuustyöhön. (Porvari 2012, 212.)

2.4 Tietosuojan merkitys liiketoiminnassa

Yrityksissä käsiteltävien henkilötietojen määrä on kasvanut ja sen myötä tarpeet tietosuojan huomioimiseen ovat lisääntyneet. Tietojärjestelmien kehittymisen myötä yritykset ovat ottaneet käyttöön uusia järjestelmiä. Tietotekniikka tuo yrityksille jatkuvasti uusia tietojen käsittelyyn perustuvia mahdollisuuksia, mutta samalla tietojenkäsittelyn ja yksityisyyden suojaamisen riskit ovat kasvaneet. (Salminen 2009, 18-19.)

Liiketoiminnan sähköistyessä tietojenkäsittelyn pelisäännöt ovat kehittyneet ja tulleet monipuolisemmiksi, mutta lainsäädäntö on vielä nuorta verrattuna moneen muuhun lainsäädännön alueeseen. Tietosuojaan liittyvän lainsäädännön vaikutus yrityksissä kasvaa sitä mukaa kun uusia sähköisen liiketoiminnan teknologioita otetaan käyttöön ja asiakastietojen käsittelyn merkitys liiketoiminnassa tulee entistä tärkeämmäksi. (Salminen 2009, 20.)

Sähköisen viestinnän tietosuojalakiin tuli uusia säännöksiä 1.6.2009. Lakimuutos antoi työnantajille oikeuden tutkia tiettyjen edellytysten täyttyessä muun muassa sähköpostiliikenteen tunnistamistietoja. Sähköisen viestinnän tietosuojalakia käsiteltiin vuonna 2009 runsaasti eri medioissa. Käytännössä lakiin tehdyt muutokset eivät kuitenkaan tuoneet suuria muutoksia monessa yrityksessä jo vallinneisiin käytäntöihin. (Andreasson & Koivisto 2013b, 142.) Media reagoi nykyään herkästi yritysten aiheuttamiin yksityisyyden loukkauksiin tai havaitsemaansa laittomaan henkilötietojen käsittelyyn. Yritykselle tällainen julkisuus voi olla hyvinkin haitallista. Kolhu yrityksen imagossa voi vaikeuttaa tuotteiden myyntiä kuluttajille ja aiheuttaa asiakaskunnassa että muissa sidosryhmissä liiketoiminnan kannalta negatiivisia reaktioita. (Salminen 2009, 20.)

Sähköisen liiketoiminnan menestyksen edellytyksenä on että asiakkaat luottavat sähköisesti toimivaan yritykseen ja uskaltavat antaa tietonsa yritykselle. Hyvän liiketoiminnan edellytyksenä on asiakkaiden luottamus yritykseen ja yrityksen vastuullisesta imagosta on tässä hyötyä. Yritys joka pystyy osoittamaan asiakkailleen toimivansa heidän yksityisyytensä suojaamisessa vastuullisesti ja luotettavasti, saa itselleen merkittävän kilpailuedun suhteessa niihin yrityksiin, jotka eivät tätä asiaa huomioi. (Salminen 2009, 21.)

Asiakasrekisterin sisältämän tiedon arvo on usein merkittävä osa yrityksen taloudellista arvoa. Yrityksen asiakastietojen ja -rekisterien merkitystä voidaan arvioida pohtimalla asiakastietojen uudelleenhankinta-arvoa. Asiakastietojen arvoa voidaan punnita esimerkiksi miettimällä kuinka paljon yritykselle maksaisi hankkia asiakkuudet uudelleen, jos nykyiset asiakastiedot eivät olisi enää käytettävissä. Asiakkaiden yksityisyyden suojaamisesta on huolehdittava. Tietosuojan oikeanlainen vastuullinen hoitaminen tuo lisäarvoa sekä yritykselle että yrityksen asiakkaille. (Salminen 2009, 22 - 23.)

3 Tietoturvallisuuden johtaminen ja hallinnointi

Tietoturvallisuus ja sen johtaminen ovat varsin laajoja käsitteitä, joilla on monia merkityksiä. Suppeimmillaan tietoturvallisuuden johtaminen tarkoittaa tietoturvallisuudesta huolehtimista lain vaatimusten edellyttävällä tavalla ilman selkeätä suunnitelmaa tai vastuuta. Laajemmin käsitettynä se tarkoittaa nimettyä tietoturvapäällikköä, jonka tehtävänä on tietoturvan hallinnointi kokonaisuudessaan. Tietoturva tulisi huomioida yrityksen kaikissa toiminnoissa osana johtamista ja sen on oltava osa työntekijöiden päivittäistä työntekoa. Tietoturvallisuus on mahdollista saada osaksi työntekijöiden jokapäiväistä toimintaa, kun se sisällytetään osaksi työntekijän normaaleja rutiineja. (Laaksonen ym. 2006, 115.)

3.1 Tietoturvallisuuden johtaminen

Yrityksen johto on keskeisessä asemassa tietoturvallisuuden ylläpitämisessä ja kehittämisessä. Ilman johdon tukea tietoturvatyö ei voi saavuttaa sille asetettuja tavoitteita. Yhteiskunnan keskeiset toiminnot ja palvelut ovat sähköistymässä ja samalla myös tietoturvauhkat painottuvat yhä enemmän tietoverkkoihin. Yrityksen johdon tulee varmistaa, että organisaatiossa on tunnistettu sitä koskeva keskeinen tietoturvaan liittyvä lainsäädäntö ja että organisaatio täyttää sille asetetut tietoturvavaatimukset. (Valtiovarainministeriö 2008, 14.)

Yrityksen johdon vastuulla on saada henkilöstö ymmärtämään tietoturvan merkitys yrityksen liiketoiminnalle ja maineelle. Johdon tapa toimia ja työskennellä ovat muille esimerkkejä siitä miten tietoturvaan yrityksessä yleisesti suhtaudutaan. Kun johto on sitoutunut tietoturvariskien hallintaan, niiden torjuminen onnistuu paremmin koko yrityksessä. (Laaksonen ym. 2006, 258 - 259.)

Tietoturvariskien hallinta on osa yrityksen kokonaisriskien hallintaa. Toimiva riskienhallinta vähentää ja lieventää organisaatiota uhkaavia vahinkoja. Se on suunnitelmallista ja jatkuvaa kehittämistoimintaa uhkien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi. (Valtiovarainministeriö 2007, 23 - 24.)

3.2 Tietoturvapolitiikka

Tietoturvapolitiikan avulla yrityksen johto määrittelee tavoitteet, vastuut ja toimintalinjat. Tietoturvallisuuden merkityksen ja yleisperiaatteiden määrittely on tärkeä perusta tietoturvakulttuurin luomiselle. Tietoturvapolitiikka toimii perustana, jonka varaan erilaiset ohjeet ja tietoturvasuunnitelmat rakennetaan. Tietoturvallisuuden johtaminen on osa kaikkea muuta johtamista ja ainoastaan yrityksen johdon sitoutuminen tietoturvallisuuden kehittämiseen mahdollistaa toiminnalle asetettujen tavoitteiden saavuttamisen. (Valtiovarainministeriö 2007, 25 - 27.)

Yrityksen ylimmän johdon sitoutuminen tietoturvallisuusasioihin alkaa tietoturvallisuuspolitiikan laatimisesta. Ylimmän johdon sitoutumisella tarkoitetaan näkyvää osallistumista tietoturva-asioiden käsittelyyn, niin että se näkyy myös henkilöstölle. Turvallisuuteen liittyvistä asioista tulee tiedottaa henkilöstölle ja ylimmän johdon tulee noudattaa tietoturvamääräyksiä siinä missä muidenkin työntekijöiden. Mikäli johtajat laiminlyövät esimerkiksi henkilökorttien käyttämisen, ei henkilöstökään pidä niiden käyttämistä välttämättömänä. (Laaksonen ym. 2006, 129 - 130.)

Yrityksen tietoturvariskejä on hallittava samanaikaisesti usealla eri organisaatiotasolla. Esimiesten tulee hallita päivittäisessä työssä vastaan tulevat tietoturvaan liittyvät tilanteet. Työntekijöiden täytyy ymmärtää käsittelemänsä tiedon arvo sekä yrityksen tietoturvapolitiikka ja toimintaohjeet, jotta he osaavat toimia oikein erilaisissa tilanteissa. Tietoturvariskejä kartoittaessa on tärkeää ottaa mukaan henkilöitä organisaation eri toiminnoista, koska eri toiminnoissa riskit voivat olla erilaisia. Kun tietoturvapolitiikka on luotu ja vastuu tietoturvan toteuttamisesta jaettu, tavoitteet pitää sisällyttää mukaan yrityksen päivittäiseen toimintaan. (Laaksonen ym. 2006, 120 - 121.)

Monet tutkijat korostavat, että suunnittelu kuuluu esimiehille eikä suorittavalle portaalle. Toisaalta tutkimukset ovat osoittaneet, että kun henkilöstö pääsee osallistumaan suunnitteluun, vastarinta muutosvaiheessa on vähäisempää. Tietoturvan suhteen suunnitteluun tulee ottaa mukaan myös työntekijöitä, jotta heidät saadaan sisäistämään tietoturvapolitiikka ja sen sisältämät tavoitteet mahdollisimman hyvin. (Laaksonen ym. 2006, 121 - 122.)

3.3 Tietoturvaohjelma

Tietoturvaohjelmalla tarkoitetaan niitä toimenpiteitä, joilla määrätään noudatettavista tietoturvallisuuteen liittyvistä periaatteista sekä tietoturvallisuuden organisoinnista. Tietoturvaohjelman tavoitteena on suojata tiedon luottamuksellisuus, eheys ja käytettävyys. Tietoturvaohjelman ei tarvitse olla laaja, mutta sen tulisi sisältää keskeiset linjaukset yrityksen tietoturvallisuuteen liittyville toimintatavoille. (Laaksonen ym. 2006, 128.) Yksi tietoturvaohjelman tärkeimmistä vaiheista on tietoturvallisuuden hallintaan liittyvien roolien ja vastuiden määrittely. Yrityksen tulee määritellä tarkasti keitä tietoturvallisuusohjelma koskettaa ja ketkä siitä vastaavat. Tämän lisäksi kannattaa miettiä koko henkilöstön sekä ulkopuolisten sidosryhmien roolia tietoturvallisuuden kannalta. (Laaksonen ym. 2006, 128.)

Tietoturvallisuuden johtaminen perustuu määrätietoiseen ja organisoituun toimintaan. Yrityksen tietoturvaohjelman laajuus riippuu sitä uhkaavista tekijöistä sekä liiketoiminnan ja toimintaympäristön vaatimuksista. Yksi tärkeitä toimenpiteitä tietoturvallisuuden johtamisessa on organisaation liiketoiminnan tavoitteiden ja tietoturvatavoitteiden yhtenäistäminen siten, että ne ovat linjassa. Tavoitteiden yhtenäistäminen lisää todennäköisyyttä sille, että organisaatio käyttää sopivan määrän oikeita resursseja tärkeisiin kohteisiin. Tavoitteiden yhtenäistämisen tuloksena voidaan myös tunnistaa liiketoiminnan kannalta merkittävimmät tietoturvakysymykset ja paneutua niihin tarkemmin. (Laaksonen ym. 2006, 117 - 118.)

Tietoturvaa uhkaavat tilanteet voivat johtua monenlaisista syistä. Ihminen voi aiheuttaa tahallaan tai tahattomasti häiriötilanteita, tietojärjestelmät voivat toimia väärin tai puutteellisesti ja tekniset suojauskeinot voivat pettää tai olla väärin mitoitettuja. Tietoturvaa uhkaavat tilanteet on syytä selvittää jo etukäteen huolellisesti, jotta mahdollisilta vahingoilta voidaan välttyä tulevaisuudessa. Tietoturvaohjelman tehtävä on kehittää yrityksen käyttöön tietoturvaohjeita ja toimintamalleja sekä teknisiä suojautumiskeinoja tietojenkäsittelyn turvaamiseksi. (Laaksonen ym. 2006, 119 - 120.)

3.4 Käyttöoikeuksien hallintaprosessi

Käyttöoikeuksien hallintaprosessi on yksi keskeisistä tietoturvallisuuteen liittyvistä prosesseista. Prosessin periaate on yksinkertainen: käyttäjille annetaan ne oikeudet, jotka he työtehtävissään tarvitsevat. Käyttöoikeuksien hallinnasta on kuitenkin usein löydetty puutteita tietoturva-arvioinneissa. Järjestelmissä voi olla käyttäjiä, jotka eivät enää ole yrityksen palveluksessa tai tunnukset saattavat olla monen henkilön yhteiskäytössä. Joskus tunnuksista ei voida selvittää ovatko käyttäjien käyttöoikeudet asianmukaiset, koska eri käyttöoikeuksien rooleja ja tarpeita ei ole huomioitu. (Laaksonen ym. 2006, 151.)

Käyttöoikeuksien hallinnan lähtökohtana tulee olla asiaa koskeva lainsäädäntö ja yrityksen omat ohjeet ja määräykset. Käyttäjien oikeudet ja oikeuksien hallinta pitää määritellä. Yleensä kannattaa ensin määritellä käyttäjäroolit ja se, mihin toimintoihin näiden roolien haltijoilla on oikeudet. Tämän jälkeen määritellään, mikä on kunkin käyttäjän rooli. Työntekijällä tulee olla käyttöoikeudet vain niihin tietoihin, jotka ovat tarpeen hän työtehtävissään. Käyttöoikeuksien selkeän hallinnoinnin lisäksi yrityksen tulee varmistaa, että käyttäjät, ylläpitäjät ja esimiehet osaavat kiinnittää huomiota salasanojen käsittelyyn ja laatuun. (Andreasson 2013a, 46.)

3.5 Henkilöstöturvallisuus

Henkilöstöturvallisuus koskee kaikkia yrityksen työntekijöitä ja se on luonteeltaan ennaltaehkäisevää. Henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietoja käsiteltäessä. Henkilöstöturvallisuuden merkitys tietojen turvaamiselle on keskeinen ja haasteelliseksi sen tekee ihminen. Henkilöstö käsittelee yrityksen tietoa vastaanottamalla, muokkaamalla, tallentamalla, välittämällä ja käsittelyn päättyessä tuhoamalla tietoa. Lisäksi henkilöstöllä on keskeinen rooli tietojärjestelmien ylläpidossa. (Valtiovarainministeriö 2008b, 12.)

Henkilöstö ja siitä johtuvat tietoturvatekijät voivat olla tietojen eheyden, luottamuksellisuuden ja käytettävyyden uhkana. Uhkana pidetään henkilöstön aiheuttamia tahallisia tai tahattomia vahinkoja, mutta myös organisaation rakenteella ja panostuksella tietotekniikkaan on suuri merkitys. Teknisten menetelmien käytön lisäksi henkilöstöllä on suuri rooli tietoturvallisuuden toteutumisessa. Henkilöstöturvallisuus on usein huomi-

oitu puutteellisesti yritysten kokonaistietoturvaa huomioitaessa. Henkilöstöhallinnon merkitystä tietoturvatyössä ei pidä väheksyä. Henkilöstöturvallisuustyössä on keskeistä suunnitelmallinen henkilöstön kehittäminen, johtaminen ja henkilöstöasioiden hallinto. (Valtiovarainministeriö 2008b, 13-14,19.)

Henkilöstöturvallisuustyöllä pienennetään henkilöstöstä aiheutuvia tietoturvariskejä muun muassa ohjeistuksella, koulutuksella, työmenetelmien kehittämisellä ja asenteisiin vaikuttamalla. Tietoturvallisuuden tulee näkyä myös yrityksen arjessa. Henkilöstön tahallisten väärinkäytösten mahdollisuus on minimoitava esimerkiksi taustaselvitysten, huolellisen tietojenluokittelun, raportoinnin, sisäisen valvonnan ja tarkastusten, kulunhallinnan ja oikeanlaisten seuraamusmenettelyjen avulla. (Valtiovarainministeriö 2008b, 20.)

Henkilöstöriskien hallinnassa käytetään useita menetelmiä. Lähtökohtina ovat tietoaineistoturvallisuus ja hallinnollinen turvallisuus, mutta myös työprosessit tulee suunnitella sellaisiksi, että henkilöstön tahallisia ja tahattomia virheitä voidaan välttää. Yleisperiaatteena pidetään sitä, että tiedot on luokiteltu asianmukaisesti ja henkilö saa vain omiin työtehtäviinsä liittyviä tietoja. (Valtiovarainministeriö 2008b, 21.)

Henkilöstöturvallisuudesta huolehtiminen alkaa rekrytoinnin yhteydessä taustatarkastusten ja mahdollisten turvallisuusselvitysten avulla. Henkilön aiheuttamien riskien kartoittamisessa on arvioitava henkilön luotettavuutta, vastuullisuutta ja osaamista. Henkilön sopivuuden arviointi pitää sisällään henkilön arvioinnin ja taustaselvitykset sekä mahdollisen viranomaisen tekemän turvallisuusselvityksen. Henkilön arvioinnin tarkoituksena on selvittää henkilön kykyä vastata työtehtävän asettamiin osaamis- ja luotettavuusvaatimuksiin. Arvioinnissa voidaan huomioida työtehtäviin liittyvien säädösten tunteminen, henkilön koulutustaso, henkilön perehtyneisyys tehtävään, henkilön aiempi kokemus ja työhistoria, suosittelijoiden lausunnot sekä henkilön saama tietoturvakoulutus. (Valtiovarainministeriö 2008b, 38.)

Viranomaisen kanssa yhteistyössä tehtävällä turvallisuusselvityksellä työnantaja pyrkii henkilöstöturvallisuuden varmistamiseen. Selvitys voi olla tarpeellinen turvallisuuden kannalta kriittisissä työtehtävissä. Turvallisuusselvitys ei itsessään sisällä arviota henki-

lön luotettavuudesta tai sopivuudesta, mutta selvityksellä saatavia tietoja voidaan käyttää yhtenä tekijänä rekrytoinnin kokonaisarvioinnissa. (Valtiovarainministeriö 2008, 40.)

Keskuskauppakamarin ja Helsingin seudun kamarin vuonna 2012 tekemän tutkimuksen mukaan kolmannes (32%) suomalaisyrityksistä on selvittänyt palkattavan henkilön taustaa. Taustaselvitysten määrä on pysynyt samana vuoden 2005 tutkimukseen verrattuna. Taustaselvitysten rajalliseen määrään vaikuttaa olennaisesti se, että niin sanottuja turvallisuusselvityksiä voi tällä hetkellä tehdä vaan tietyin ehdoin. Taustaselvitykset ovat erityisen tärkeitä avainhenkilöitä palkatessa, koska heillä on usein hallussaan yrityksen toiminnan kannalta tärkeää tietoja ja laajat käyttö- ja kulkuoikeudet. Jos turvallisuusselvitystä ei voida tehdä, henkilön taustaa voi selvittää ottamalla yhteyttä hakijan antamiin suosittelijoihin. (Keskuskauppakamari & Helsingin seudun kamari 2012, 20.)

3.6 Henkilöstön kouluttaminen ja ohjeistus

Ihmisten käyttäytymiseen on laadittu useita malleja, joita on sovellettu myös henkilöstön tietoturvakäyttäytymiseen. Tietojenkäsittelyn ja tietoturvariskien hallinta vaatii organisaation luonteen ja kulttuurin ymmärtämistä sekä näkemystä siitä, miten erilaiset toimintatavat voivat vaikuttaa henkilöstön käyttäytymiseen. (Laaksonen ym. 2006, 248.) Henkilöstön ei tarvitse tietää kaikkea tietoturvasta, vaan riittää että jokainen ymmärtää omaan työhönsä liittyvät riskit ja tietää miten ne minimoidaan. Teknisten tietoturvaratkaisujen tulisi näkyä käyttäjille mahdollisimman vähän tai ei ollenkaan. Ohjeiden antamisen lisäksi on korostettava riittävästi toimintatapojen perimmäisiä syitä, jotta henkilöstö ymmärtää syyt eikä pidä ohjeita pelkästään byrokraattisina. (Laaksonen ym. 2006, 254 - 255.)

Henkilöstön tietoturvakäyttäytymiseen liittyy organisaation näkökulmasta kolme asiaa: tietoturvaohjeet ja koulutus, työyhteisön näyttämä esimerkki ja työntekijän oma maalaisjärki. Päivittäisten työtehtävien suorittamisessa työntekijät ottavat mallia toisiltaan ja myös työntekijän aikaisempi kokemus ja osaaminen vaikuttavat päätöksentekotilanteisiin. Tietoturvapolitiikka ja -ohjeet luovat rungon henkilöstön toimintatavoille. (Laaksonen ym. 2006, 248 - 249.)

Tietoturvallisuudessa tarvitaan muita toimintoja enemmän yhdenmukaisia ja yhteensopivia toimintaohjeita. Yleisluontoisella ohjeistuksella saavututetaan vain harvoin henkilöstön sitoutuminen turvallisiin toimintatapoihin. Varsinaisen ohjeistuksen tuleekin koostua omaan organisaatioon ja sen toimintatapaan sovitetuista ja yrityksen omaan tietoturvapolitiikkaan perustuvista ohjeista. Ohjeet tulee sijoittaa niin että ne ovat helposti saatavilla kaikille niitä tarvitseville. (Valtiovarainministeriö 2007, 49). Tietoturvaohjeistus ei voi antaa vastausta jokaiseen tilanteeseen, vaan jokaisen työntekijän tulee soveltaa ohjeita käytännön työssään. Suurin osa turvallisuuspäätöksistä tehdään vakaassa toimintaympäristössä, joka voi kestää suuriakin virhearviointeja. Henkilöstölle muodostuu taito tehdä nopeita päätöksiä ohjeiden mukaisesti vasta kokemuksen myötä. Kouluttamalla henkilöstöä toimimaan oikein ja valvomalla ohjeiden noudattamista, voidaan inhimillisestä toiminnasta aiheutuvien riskien todennäköisyyttä pienentää. (Laaksonen ym 2006, 252.)

Henkilöstön tietoturvaosaamisen suhteen yrityksen on varmistuttava siitä, että henkilöstö on koulutettu tunnistamaan ja noudattamaan yrityksen tietoturvakäytäntöjä. Ohjeiden laatiminen ei yksin riitä tietoturvan ja päivittäisen työskentelyn yhdistämiseen. Tietoturvaohjeita laadittaessa on tunnistettava mihin käyttöön ne tulevat ja keitä ohjeet koskevat. Lisäksi tulee miettiä, miten työntekijät saadaan lukemaan ja noudattamaan ohjeita. (Laaksonen ym. 2006, 160 - 161.)

Tietoturva-asiantuntijat ovat kohdanneet vaikeuksia henkilöstön huomion kiinnittämisessä turvallisuuteen. Ihmisten kohteliaisuus tekee monet turvallisuusjärjestelmät hyödyttämiksi kun ovia avataan tuntemattomille ja avaimia lainataan esimerkiksi arkistokaappien avaamiseen. Turvallisuustason kohottaminen vaatii muutoksia ihmisten käyttäytymisessä. Ihmisten käyttäytymisen ennustaminen ja ymmärtäminen on tärkeää tietoturvallisuuden kehittämisessä. Tietoturvasta vastaavien tahojen on ymmärrettävä asiat, jotka vaikuttavat henkilöstön tapaan muodostaa kuva yrityksessä vallitsevasta käytännöstä. (Laaksonen ym. 2006, 252 - 253.)

Tietoa käsitteleville työntekijöille on korostettava, että heidän käsittelemä tieto on yrityksen toiminnan kannalta arvokasta. Luokittelun avulla täsmennetään tiedon merkitystä liiketoiminnalle, selkeytetään tiedon käsittelyä ja korostetaan henkilöstölle tiedon

merkitystä. Tietojen luokittelussa määritellään tiedon tärkeysluokka, tiedon käsittelyn periaatteet, tiedon salaamiseen ja tiedon hävittämiseen liittyvät asiat. Mikäli yrityksessä tuotetaan ja käsitellään paljon arkaluontoista tietoa paperimuodossa, tulisi niitä varten olla erilliset paperinkeräysastiat ettei arkaluontoista tietoa ei pääse normaaliin keräysastiaan. (Laaksonen ym. 2006, 161.)

Keskuskauppakamarin ja Helsingin seudun kamarin tutkimuksen mukaan 53 % yrityksestä kouluttaa henkilökuntaansa salaisten tai luottamuksellisten tietojen käsittelyyn. Suurissa yrityksissä koulutus on yleistä (71 %), kun taas pienistä yrityksissä vain puolet (50 %) kouluttaa henkilökuntaansa näissä asioissa. Tutkimuksen perusteella suomalaisten yritysten olisi syytä panostaa vielä nykyistä enemmän kriittisten tietojen tunnistamiseen ja suojaamiseen esimerkiksi koulutuksen avulla. Koulutuksen antama osaaminen voi jossain tilanteessa olla ainoa asia, joka estää luottamuksellisen tietojen päätymisen vahingossa vääriin käsiin. Koulutus parantaa työntekijöiden turvallisuusosaamista ja vähentää yrityksen tai asiakkaiden tietoihin kohdistuvia uhkia. (Keskuskauppakamari & Helsingin seudun kamari 2012, 30.)

4 Tietoturvan tekninen toteuttaminen

Ohjeistus ja muu tietoturvadokumentaatio muodostavat merkittävän osan tietoturvallisuuden käytännön toteuttamisesta. Tämä ei kuitenkaan riitä vaan niiden lisäksi ja tueksi tarvitaan myös teknisiä keinoja. Tietoturva on parhaimmillaan silloin, kun se on osa jokapäiväistä toimintaa ja toimii taustalla niin ettei käyttäjien tarvitse murehtia tietoturvan toimivuutta. Oikein suunniteltuina ja toteutettuina tekniset suojauskeinot tarjoavat mahdollisuuden tällaiseen tietoturvan toteuttamiseen. Teknisiä suojauskeinoja ovat virustorjuntaohjelmistot, palomuurit, tunkeutumisen esto, tietojen salaus ja roskapostin suodatus. (Laaksonen ym. 2006, 172.)

4.1 Haittaohjelmat ja niiden torjunta

Haittaohjelmalla tarkoitetaan yleensä sovellusta, jonka tarkoituksena on aiheuttaa tietojärjestelmässä tapahtumia, joita käyttäjä ei ole aikonut suorittaa. Haittaohjelmia torjuttaessa yrityksen ohjeistuksessa tulisi ottaa huomioon mitä haittaohjelmat tekevät, miten käyttäjä voi toiminnallaan välttää haittaohjelmia ja miten käyttäjän tulee toimia epäillessään tietokoneensa sisältävän haittaohjelman. Lisäksi henkilöstöä tulisi selkeästi ohjeistaa, ettei tietynlaisia liitteitä tai viestejä pidä avata eikä tällaisia viestejä tule lähettää edelleen. (Laaksonen ym. 2006, 163.)

Lacey ja James (2010) ovat katsauksessaan todenneet, että pk-yritykset eivät turvaa riittävästi arkaluonteisia tietojaan. Syyksi tietoturvan puutteille he kertovat muun muassa sen että pk-yritykset pitävät tietoturva-asioita muiden ongelmana, eivätkä näe omissa tiedoissaan mitään varastettavaa. Myös Heljaste ym. (2008, 71-72) toteavat, että käyttäjä saattaa ajatella ettei hänen tiedoissaan ole mitään varastamista. Haittaohjelmien tekijät eivät välttämättä olekaan varastamassa dataa. Kaikissa tietokoneissa on nykyisten laajakaistayhteyksien aikana kuitenkin varastettavana ainakin prosessoritehoa ja vapaata levytilaa. Verkkorikolliset kaappaavat tietokoneista haltuunsa haittaohjelmien avulla käyttääkseen niitä esimerkiksi roskapostin välittämiseen tai laittomien ohjelmien jakamiseen. Viestintäviraston mukaan Suomessa on kokoajan tuhansia koneita mukana tällaisissa bottiverkoissa.

Haittaohjelmia torjutaan muun muassa virustorjuntaohjelmistoilla. Työasemien virustorjunta on yleensä hoidettu suomalaisissa yrityksissä hyvin. Työasemien lisäksi virustorjunta tulee järjestää myös palvelinympäristölle, kannettaville laitteille ja internetliikenteelle. Lisäksi on tärkeää ohjeistaa käyttäjiä erityisesti sähköpostin ja internetin käytössä. (Laaksonen ym. 2006, 204-205.)

Tunkeutumisen havaitsemis- (IDS) ja estämisjärjestelmät (IPS) on tarkoitettu valvomaan verkkoa ja verkossa olevia laitteita sekä estämään tai ainakin havaitsemaan haitallisia tapahtumia. Järjestelmien toiminta perustuu normaalista poikkeavan liikenteen tunnistamiseen tietoverkossa. IDS- ja IPS -järjestelmien käyttöönotto tulee aina tehdä harkiten ja järjestelmien säätämiseen tulee kiinnittää tarpeeksi huomiota. Tärkeintä on saada järjestelmä säädetyksi niin, että hälytysten määrä on mahdollisimman pieni, mutta mitään merkittäviä tekijöitä ei jää huomiotta. (Laaksonen ym. 2006, 190.)

Tietoturvaohjelma kannattaa valita koneen käyttötarkoituksen ja yrityksen koon mukaan. Yhden hengen yritykseen saaatetaan tarvita erilaiset ohjelmat kuin suurempaan yritykseen. Yrityksen ei tarvitse olla kovinkaan suuri kun se tarvitsee jo keskitettyä hallintaa tietoturvan ylläpitoon. Käyttöjärjestelmän ja tietoturvaohjelmiston päivityksistä tulee huolehtia ja molemmat päivitykset voi yleensä helposti automatisoida. Muiden ohjelmien päivitysten osalta riittää kohtuullinen varmuus. (Heljaste ym 2008, 83.)

4.2 Palomuurit

Palomuuriohjelmistot antavat hyvän suojan tietomurtoja vastaan. Palomuurien toinen tehtävä on suojata konetta internetistä tulevia uhkia vastaan. Uudemmissa käyttöjärjestelmissä on jo valmiiksi mukana ainakin jonkinlainen palomuuri ja myös lähes kaikki tietoturvaohjelmistot sisältävät palomuuriominaisuuden. Palomuuria ei tarvitse yleensä konfiguroida mitenkään, vaan oletusasetuksilla pärjää hyvin kun huolehtii siitä että palomuuri on asennettu ja se pidetään päällä. Yrityksen oma verkko on suositeltavaa suojata erillisellä palomuurilla ja eristää se julkisesta verkosta eli internetistä. (Heljaste ym. 2008, 75.)

4.3 Etätyö ja kannettavien laitteiden tietotuva

Etätyöllä tarkoitetaan muualla kuin yrityksen omassa toimipisteessä tehtävää työtä. Tyypillisesti etätyö on kotona tehtävää toimistotyötä, mutta käyttöympäristö voi myös vaihdella. Työntekijän omilla työtavoilla on tällöin suuri merkitys. Etäyhteys on tietoliikenneyhteys yrityksen sisäverkon ulkopuolelta yrityksen omaan verkkoon. Langattomien yhteyksien yleistyessä työntekijän on etätyötä tehdessään osattava arvioida itsenäisesti etätyöympäristön turvallisuutta. Etätyössä tulee noudattaa samoja turvallisuusohjeita kuin organisaation varsinaisissa tiloissa. (Andreasson 2013a, 52.)

Yrityksen käytössä olevien tietojenkäsittelylaitteiden määrä on kasvanut ja etätyössä käytettävä laite voi olla kannettava tietokone, älypuhelin tai tablettitietokone. Etätyöhön liittyvissä ratkaisuissa on jo ennen toteutusta määriteltävä tietoturvaan ja tietosuojaan liittyvät asiat huolellisesti. Etätyössä riskejä ovat muun muassa laitteiden häviäminen tai joutuminen vääriin käsiin sekä haittaohjelmat, joiden avulla voidaan pahimmassa tapauksessa päästä tunkeutumaan suoraan yrityksen sisäverkkoon. Älypuhelimet tulee suojata esimerkiksi suojakoodeilla, jotka lukitsevat puhelimen automaattisesti tietyn ajan kuluttua. (Andreasson 2013a, 54.)

Kannettava tietokone on kiinnostava kohde varkaalle. Laite on itsessään helppo myydä eteenpäin ja sen sisältämä tieto voi myös olla arvokasta. Kannettavaa tietokonetta tai puhelinta ei tule pitää esillä esimerkiksi auton takapenkillä. Tietokonevalmistaja Dellin teettämän tutkimukseen osallistuneista puolet ilmoitti säilyttävänsä koneellaan yrityksen luottamuksellisia tietoja, mutta suurimmassa osassa tapauksista tietoja ei ole suojattu varkauden tai katoamisen varalta. (Heljaste ym 2008, 73.)

Laitteen menetys ei tavallisesti ole taloudellisesti merkittävä tappio menetettyyn tietoon verrattuna. Vaikka laitteiden suojaamiseen käytetään salasanoja, ei tieto välttämättä ole turvassa laitteen katoamisen jälkeen. Salaamalla kannettavan tietokoneen kiintolevy voidaan estää ulkopuolisten tahojen pääsy koneelle tallennettuihin tietoihin esimerkiksi varkaustapauksen yhteydessä. Kannettavien laitteiden käytön ohjeistamisessa tulisi huomioida missä laitetta tullaan käyttämään ja mitä tietoa laitteessa säilytetään. Arka-

luontoinen tieto on suojattava asianmukaisesti. Tietojen varmuuskopioinnista on myös huolehdittava. (Laaksonen ym. 2006, 168; 196.)

Kannettavien laitteiden tietoturvallisuuden tekevät haasteelliseksi vaihtuvat käyttöympäristöt, joiden fyysistä tietoturvaa ei voida varmistaa. Tämän vuoksi laitteella olevien tietojen salaamisesta tulee huolehtia. Tämä kannaattaa toteuttaa kiintolevyn salaavalla ohjelmistolla, joka on yrityksen ICT-tuen keskitetyssä hallinnassa. Kannettavia laitteita käyttäessä myös tietoliikenneyhteydet voivat olla eri tavoin toteutettuja. Päätelaite on suositeltavaa varustaa joko kaiken tietoliikenteen automaattisesti salaavalla ratkaisulla tai salata tietoliikenne ohjelmittain. Tarvittaessa tulee huolehtia myös vahvasta käyttäjän ja päätelaitteen tunnistamisesta. (VAHTI 2012, 45.)

Työnantaja hoitaa pääsääntöisesti etäkäytössä vaadittavien laitteiden, ohjelmistojen ja tietoliikenneyhteyksien hankinnan ja asentamisen. Työntekijän on huolehdittava siitä että etätyössä käytetyt laitteistot, ohjelmistot ja yhteydet ja paperiaineistot pysyvät ainoastaan hänen omassa käytössään. Sama koskee etätyössä käytettäviä käyttäjätunnuksia, salasanoja ja mahdollisia toimikortteja ja muita todennusvälineitä. Etätyöntekijän tulisi kuljettaa mukanaan vain välttämätön määrä tietoaineistoa ja varmistettava aina että aineisto on asianmukaisesti suojattu. (Andreasson 2013a, 53.)

Liitettäessä kone julkiseen verkkoon työpaikan ulkopuolella, on muistettava koneessa olevan virustorjuntaohjelmiston ja palomuurin lisäksi huolehtia tiedonsiirron tietoturvasta. Tällöin kyseessä on VPN:n (Virtuel Private Network) käyttö. VPN luo salakirjoitetun tunneloidun yhteyden yrityksen omaan verkkoon, jolloin tietoa ja sähköpostia voidaan siirtää julkisen verkon eli internetin yli. Sähköposteja ei pidä lukea internetin yli omalta sähköpostipalvelimelta ilman ilman VPN:ää eikä myöskään siirtää mitään tiedostoja toimistolta omaan koneeseen. (Heljaste ym 2008, 81.)

4.4 Sähköposti

Sähköposti on hyvä työväline yhteydenpitoon. Tulee kuitenkin muistaa, ettei sähköpostissa ole itsessään mitään suojausta oletuksena vaan tiedot liikkuvat salaamattomina

julkisessa verkossa. Sähköpostin liitetiedostot voivat sisältää haittaohjelmia kuten viruksia, matoja tai troijalaisia. Kaikkia epätavallisia sähköposteja tulee varoa ja erityisesti liitetietoja ja www-sivujen linkkejä tulee olla avaamatta. (Andreasson 2013a, 55.)

Sähköpostin käytön suurimpia ongelmia on ollut jatkuvassa kasvussa ollut roskapostin määrä ja näiden viestien vastaanottamisesta sekä torjumisesta aiheutuvat kustannukset. Roskapostia voivat olla esimerkiksi sähköpostiin tilaamatta tulleet mainokset. Roskaposteihin ei pidä vastata, vaan ne kannattaa poistaa heti. Vastaamalla viestiin kerrot roskapostittajalle että sähköpostiosoite on käytössä. Paras tapa suojautua roskapostilta on olla päätymättä roskapostittajien listalle. Työsähköpostiosoitetta ei tule antaa ulkopuolisille muissa kuin työhön liittyvissä yhteyksissä. (Andreasson 2013a, 56; 206.)

Yrityksen sähköpostiosoitteita ei tulisi ilmoittaa verkkosivuilla tai missään muualla sähköisessä muodossa. Sähköpostiosoite voidaan ilmoittaa etunimi.sukunimi@yritys.fi -muodossa tai sen voi lisätä esimerkiksi kuvatiedostona yrityksen www-sivulle. Käyttäjille tulee lisäksi järjestää riittävä ohjeistus ja koulutus sähköpostin käytöstä. Roskapostin torjuntaan käytetään merkittäviä resursseja ja torjuntatyössä vaaditaan ohjelmistoja, laitteita ja asiantuntijoiden aikaa. Lisäksi roskapostin torjunta voi haitata sähköpostin käyttöä normaaleissa työtehtävissä. Toisaalta sähköpostiliikenteen suodatus voi myös vahingossa poistaa tarpeellisia viestejä. (Laaksonen ym. 2006, 210.)

4.5 Tietojen salaus

Tietojen salauksen avulla varmistetaan tietojen luottamuksellisuuden säilyminen. Salausta hyväksikäyttävien sovellusten avulla voidaan myös varmistaa tietojen eheys sekä eri järjestelmien tai käyttäjien välisten toimenpiteiden kiistämättömyys. Salauksen avulla voidaan esimerkiksi varmistua siitä, että sähköpostin lähetti juuri oikea henkilö tai järjestelmään kirjautunut tilaus todella tuli yrityksen tietojärjestelmästä. Yrityksen käyttämän tiedon luokittelussa ja siihen liittyvässä ohjeistuksessa tulisi ottaa kantaa tietojen salaamiseen. Ohjeissa voidaan esimerkiksi sallia salaiseksi luokitellun tiedon lähettäminen ainoastaan salattuna. Kannettavien laitteiden sisältämä tieto voidaan suojata salaamalla koneen kiintolevy. (Laaksonen ym. 2006, 195-196.)

4.6 Salasanat

Käyttäjätunnukset ja salasanat ovat henkilökohtaisia, eikä niitä saa antaa toiselle henkilölle. Käyttäjätunnukseen liitetyn salasanan tulee olla vain sen käyttöön oikeutetun henkilön tiedossa. Salasanan tulee olla riittävän pitkä ja sitä tulee muuttaa tarpeeksi usein. Työntekijöille on tärkeä kertoa salasanojen käytön periaatteet hyvin yksityiskohtaisesti. Työpaikan verkkotunnuksen salasana ei saa olla sama, jota henkilö käyttää yksityiselämässään. Toisaalta henkilöstöä tulee myös varoittaa monen salasanan aiheuttamista ongelmista. Jos muistettavia salasanoja on useita, käyttäjälle tulee kiusaus kirjoittaa ne ylös. Tätä riskiä tulee pienentää suunnittelemalla tekniset järjestelmät niin, että eri käyttäjätunnusten ja salasanojen tarve vähenee. (Laaksonen ym. 2006, 166 - 167.)

Salasanoihin liittyvää ohjeistusta laadittaessa on syytä miettiä miten käyttäjät saadaan noudattamaan ohjeita. Käyttäjille tulee aina perustella ohjeiden tärkeys. Tässä auttavat esimerkit siitä mitä riskejä ohjeiden laiminlyönti saattaa aiheuttaa. Salasanaohjeistusta tehtäessä on tärkeää laatia ohjeet koskien turvallisen salasanan muodostamista, oletussalasanojen välitöntä muuttamista, salasanojen vaihtamista ja lisäksi annettava ohjeet salasanan unohtamista tai vääriin käsiin joutumista varten. (Laaksonen ym. 2006, 167.)

Henkilöstöä kannattaa ohjeistaa pitämään pöytänsä puhtaana niin, ettei papereita jää lojumaan ympäriinsä. Kiinteistöissä liikkuu yleensä ulkopuolisia tahoja kuten siivoajia ja vartioita. Vaikka ei olisi syytä epäillä näiden henkilöiden luotettavuutta, voivat he nähdä salaisia tietoja myös vahingossa, mikäli dokumentit eivät ole asiallisesti kansioissa mieluiten lukituissa kaapeissa. Yrityksen kannattaa huolehtia puhtaan pöydän periaatteesta myös yrityssalaisuuksien suojaamisen takia.
(Laaksonen ym. 2006, 170.)

4.7 Varmuuskopiointi

Yrityksen hallussa oleva tieto on varmistettava siten, että se säilyy luotettavana ja on niiden henkilöiden käytössä, jotka sitä työssään tarvitsevat. Parhaiten tämä toteutuu jos käyttäjien ei tarvitse edes tietää mitään tietojen varmistuksesta. Varmuuskopiointi on helpointa toteuttaa ohjaamalla kaikki ohjelmat keskitetysti tallentamaan varmistettaville verkkolevyille, jossa on tarpeeksi tallennuskapasiteettia. (Laaksonen ym. 2006, 170.)

Kaikkien tietojen keskitetty varmuuskopiointi ei ole aina mahdollista ja tärkeiden tietojen osalta ohjeistuksessa on otettava huomioon ainakin tärkeän tiedon varmistaminen välittömästi, tiedon säilytyspaikka, säilytystapa ja arkistointi, tietoihin pääsy, tiedostojen siirto ja palautukset. Varmistettu tieto tulee testata ja palauttaa aika ajoin, jotta voidaan varmistua siitä että varmistusprosessi toimii. Yrityksen ei kannata luottaa siihen, että työntekijät itse varmistavat omat tietonsa riittävän usein. Varmistuksen tulee siten olla käyttäjille mahdollisimman helppoa ja automaattista. (Laaksonen ym. 2006, 170 – 171.)

4.8 Pilvipalvelut

Pilvipalvelut ovat yleistyneet viime aikoina ja pilvipalveluiden turvallisuus on aiheuttanut kysymyksiä. Pilvipalveluilla tarkoitetaan mallia, jossa tietoteknisiä resursseja tarjotaan verkon välityksellä yrityksen käyttöön ilman että käyttäjän tarvitsee tietää missä ne sijaitsevat. Käyttäjän ei myöskään tarvitse huolehtia pilvipalveluiden toiminnasta tai ylläpidosta. (Salo 2010, 16.)

Perinteisen palvelinkeskuksen etuna on, että kokemusta tietoturvaongelmien ratkaisusta on runsaasti, kun taas pilvipalvelut ovat uusia ja käyttökokemusta ei vielä ole tai sitä on vähän. Tämän lisäksi osa ratkaisuvastuusta siirtyy palveluntarjoajien vastuulle, jolloin kysymys on teknisten ratkaisujen lisäksi luottamuksesta. Luottamuskysymysten lisäksi haasteelliseksi turvallisuusongelmien ratkaisemisen tekee pilvipalvelumarkkinoiden nuoruus ja pirstaleisuus. (Salo 2010, 103.)

Andreassonin ja Koiviston (2013b, 26) mukaan pilvipalvelujen joustavuus ja kustannustehokkuus tulevat johtamaan niiden merkittävään yleistymiseen. Palvelujen ja niissä olevien tiedon siirto oman verkon ulkopuolella aiheuttaa useissa huolta tietoturvallisuudesta ja Andreassonin mukaan huoli on aiheellinen, ja se pakottaa organisaation miettimään tietoturvakäytäntöjään ja sopimustensa sisältöjä. (Andreasson & Koivisto 2013b, 26.) Myös Lacey ja James (2010) ovat katsauksessaan todenneet, että pilvipalvelujen turvallisuus aiheuttaa pk-yrityksille erityisiä kysymyksiä, koska niillä ei välttämättä ole resursseja selvittää palveluiden luotettavuutta samalla tavalla kuin isommilla yrityksillä.

Andreassonin ja Koiviston (2013b, 26) mukaan keskeisiä pilvipalveluiden tietoturvan kannalta mietittäviä kysymyksiä ovat:

- Missä tiedot sijaitsevat?
- Kuinka tiedot suojataan?
- Kuka pääsee käsitelemään tietoja ja kuinka käyttöä valvotaan?
- Vastaako palvelujen tietoturva asiakkaan vaatumuksia?
- Onko riskianalyysit tehty?
- Onko tietoturva-asiat huomioitu riittävän tarkasti sopimuksissa?
- Mitkä ovat käytännön mahdollisuudet siirtyä pois käyttöön otetusta palvelusta?

5 Tutkimus

5.1 Tutkimuksen tausta

Tietoturvan merkitys on korostunut entisestään kun yhtä useammat yritykset hyödyntävät tietotekniikkaa jokapäiväisessä yritystoiminnassaan. Pk-yrityksen tietoturvasta on tehty aiemmin Suomessa muutamia tutkimuksia. Kattavimmin asiaa on tutkinut Kauppa- ja tietoturvaministeriön vuonna 2006 teettämä Pk-yritysten tietoturvakysely.

Kauppa- ja teollisuusministeriö teetti vuonna 2006 Pk-yritysten tietoturvakyselyn, joka oli ensimmäinen Suomessa tehty kattava selvitys pk-yritysten tietoturvasta. Selvityksen päätulokset vahvistivat ennakkokäsitystä pk-yritysten tietoturvan hoidosta. Tietoturvan tekninen puoli oli suurimmalla osalla yrityksistä kunnossa, mutta hallinnollisessa tietoturvassa oli parantamisen varaa. (Kauppa- ja teollisuusministeriö 2007.)

Pk-yritysten tietoturvaa selvitettiin teknisten valmiuksien ja teknisen tietoturvan, henkilöstön tietoturvatietämyksen ja hallinnollisen tietoturvan sekä tietojärjestelmiin liittyvän riskienhallinnan näkökulmasta. Tutkimuksessa selvisi että pienemmissä yrityksissä sekä tekninen tietoturva että tietoturvan inhimillinen puoli oli hoidettu heikoiten. Parhaiten tietoturva oli hoidettu keskisuurissa yrityksissä. Myös riskienhallinnassa erot mikroyritysten, pienten yritysten ja keskisuurten yritysten välillä olivat selvät. Kokonaisuudessaan kyselyn tulokset osoittivat että tarve tietoturvan parantamiseen pk-yrityksissä oli ilmeinen. (Kauppa- ja teollisuusministeriö 2007.)

Vuonna 2007 Tietotekniikan liitto ry tutki asiaa pienemmässä tutkimuksessa (220 vastaajaa) pk-yritysten tietoturvatilannetta. Tutkimuksessa kävi ilmi että suomalaiset pk-yritykset keskittyvät suojaamaan tietojärjestelmänsä pääasiassa teknisin keinoin, vaikka työntekijöiden tahattomat virheet ja tietämättömyys koetaan merkittävimpänä tietoturvaa uhkaavana tekijänä. Heikoimpana lenkkinä nähtiin työntekijät, joiden taidot ja osaaminen ei vastaa vaatimuksia. (Tietotekniikan liitto ry 2007.)

Lacey ja James toteavat katsauksessaan että pienet ja keskisuuret yritykset kohtaavat yhä enemmän tietoturvauhkia, mutta harva pk-yritys turvaa riittävästi arkaluonteisia tieto-

jaan. Katsauksen mukaan pk-yrityksillä ei ole riittäviä tietoja ja taitoja tietoturvauhkilta suojautumista vastaan ja pk-yritykset pyrkivät tyypillisesti välttämään ylimääräisiä kustannuksia tällä alueella. (Lacey & James 2010.)

5.2 Tutkimusongelma

Tämän opinnäytetyön tehtävänä on kartoittaa tärkeimpiä pk-yrityksiä koskevia tietoturvakysymyksiä ja löytää niihin ratkaisuja. Projektiin liittyvän tutkimuksen tarkoituksena oli löytää vastaus kysymykseen: Mikä on tämänhetkinen tietoturvan taso kohderyhmän yrityksissä? Pk-yrityksen tietoturva on kokonaisuudessaan hyvin laaja alue, joten tutkimuksessa päätettiin keskittyä tutkimaan tärkeimmiksi ja ajankohtaisimmiksi koetuja tietoturvan osa-alueita. Kysymysten aihealueiksi valikoitui edellä mainitun perusteella tekniset tietoturvaratkaisut, henkilöstöön liittyvä tietoturva, liiketoimintaan liittyvä tietoturva ja salasanojen käyttötottumukset. Lisäksi avoimilla kysymyksillä kysyttiin yrityksen suurimpia puutteita tietoturva-asioissa ja annettiin vastaajille mahdollisuus tarkentaa vastauksia tai kertoa vapaasti näkemyksiään tietoturvaan liittyen. Tutkimukseen valituilla kysymyksillä pyrittiin selvittäämään kohderyhmän tietoturvan tasoa keväällä 2013.

Tutkimuskysymykseen lähdettiin etsimään vastausta toistamalla Kauppa- ja teollisuusministeriön vuonna 2006 teettämän tutkimuksen tietotekniseen tietoturvaan, henkilöstöturvallisuuteen ja liiketoimintaan liittyviä kysymyksiä. Pyrkimyksenä oli myös selvittää, onko pk-yritysten tietoturvassa tapahtunut muutoksia vuoden 2006 tutkimustuloksiin verrattuna. Tämän lisäksi tutkimuksessa toistettiin myös tietoturvaratkaisuja koskeva kysymys Tietotekniikan liitto ry:n 2007 teettämästä tutkimuksesta. Edellämainittujen aiemmista tutkimuksista toistettujen kysymysten lisäksi tutkimukseen sisällytettiin salsasanojen käyttötottumuksia kartoittava kysymys sekä kaksi avointa kysymystä tietoturvaan liittyen.

5.3 Tutkimuksen kohderyhmä

Tutkimuksen kohderyhmäksi valittiin suomalaiset pk-yritykset. Pk-yrityksen määritelmänä käytettiin Tilastokeskuksen vakiintunutta luokittelua:

Yritysluokka	**Henkilökunta**
Mikroyritys	<10
Pieni yritys	10-49
Keskisuuri yritys	50-249

5.4 Tutkimusmenetelmät

Tutkimus toteutettiin kvantitatiivisena eli määrällisenä tutkimustyönä. Aineiston keräystavaksi valittiin kysely, jonka etuna pidetään sitä, että sen avulla voidaan kerätä laaja tutkimusaineisto. Tutkimukseen voidaan saada mukaan paljon henkilöitä ja siinä voidaan myös kysyä monia asioita. Kyselymenetelmä on tehokas ja se säästää aikaa ja vaivannäköä. (Hirsjärvi, Remes & Sajavaara 2010, 195.)

Tutkimuksella on aina jokin tarkoitus tai tehtävä. Tässä tutkimuksessa tutkimusongelma on luonteeltaan kartoittava. Kartoittavan tutkimuksen tarkoitus on selvittää mitä tapahtuu, etsiä uusia näkökulmia, löytää uusia ilmiöitä, selvittää vähän tunnettuja ilmiöitä ja kehittää hypoteeseja. Tällä tutkimuksella kartoitetaan pk-yritysten tietoturvan tasoa ja etsitään mahdollisesti uusia esiin tulevia ilmiöitä, joista pk-yritysten edustajat kaipaavat lisätietoja. Lisäksi kartoitetaan ovatko toistettujen kysymysten vastaukset muuttuneet verrattuna vuosina 2006 ja 2007 tehtyihin tutkimuksiin. (Hirsjärvi ym. 2010, 137-138.)

Kysely pyrittiin luomaan selkeäksi, jotta siihen vastaaminen olisi mahdollisimman helppoa ja vastausprosentti pysyisi korkeana. Kysely koostui monivalintakysymyksistä ja avoimista kysymyksistä. Kyselyn vastaamisprosentin nostamiseksi mihinkään kysymykseen ei edellytetty pakollista vastausta.

5.5 Tutkimuksen toteutus

Kysely (Liite 1) toteutettiin Webropol-ohjelmistolla luodulla internetkyselyllä. Tutkimuksen kysymykset pyrittiin valitsemaan niin että aihe pysyisi rajattuna, mutta kysymykset toisivat silti mahdollisimman perusteellisen vastauksen tutkimuskysymykseen. Tutkimus pyrittiin pitämään lyhyenä ja ytimekkäänä, että siihen saataisiin mahdollisimman paljon vastauksia.

Kyselyn alussa (kysymykset 1-3) kysyttiin yrityksen kokoa, toimintavuosia ja liikevaihtoa. Liikevaihtoa kysyttiin lähinnä yrityksen koon todentamiseksi.

Kysymys 4 koski yrityksen käyttämiä tietoturvaratkaisuja ja se toistettiin sellaisenaan Tietotekniikanliitto ry:n vuonna 2007 teettämästä tutkimuksesta.

Kysymykset 5-7 toistettiin sellaisinaan Kauppa- ja teollisuusministeriön vuoden 2006 tutkimuksesta. Kysymyksessä 5 kysyttiin yritysten teknisten tietoturva-asioiden hoitoa, kysymyksessä 6 henkilöstöön liittyviä tietoturva-asioita ja kysymyksessä 7 liiketoimintaan liittyviä tietoturva-asioita.

Viimeiset kolme kysymystä luotiin täydentämään tutkimusta, koska niiden aiheet katsottiin ajankohtaisiksi ja tärkeiksi tutkimusongelman vastaamisen kannalta. Kysymys 8 koski salasanojen käyttötottumuksia ja se lisättiin omaksi kysymyksekseen aiheen tärkeyden ja ajankohtaisuuden vuoksi. Kysymys 9 oli avoin kysymys, jossa kysyttiin yrityksen mielipidettä suurimmista puutteistaan tietoturva-asioissa. Viimeisessä kysymyksessä numero 10 vastaajalla oli vielä mahdollisuus tarkentaa vastauksiaan tai kertoa vapaasti näkemyksiään tietoturva-asioihin liittyen.

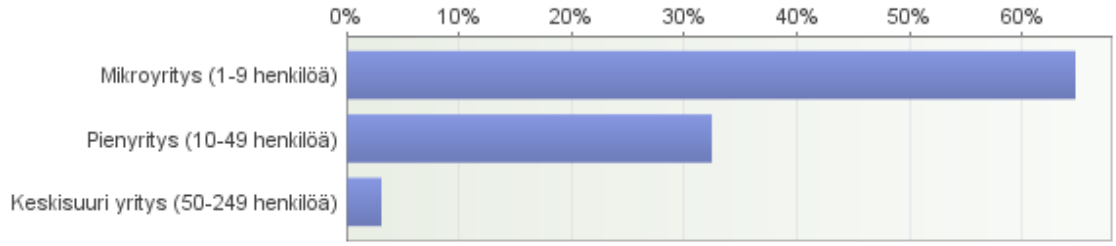
Kyselylomake esitestattiin kahden tietoturvaan perehtymättömän henkilön toimesta ja siihen tehtiin tarvittavat muutokset heidän kommentiensa perusteella.
Linkki kyselyyn lähetettiin noin 450:lle satunnaisesti valitulle pk-yrityksen edustajalle ja lisäksi linkki lisättiin Suomen Yrittäjät ry:n Facebook-sivulle ja Yrittäjät24 -keskustelupalstalle. Kysely oli vastattavana internetissä 6.-14.5.2013.

6 Tutkimustulokset

Kyselytutkimukseen vastasi 65 pk-yrityksen edustajaa. Tarkkaa vastausprosenttia ei voida määrittää, koska linkki kyselyyn oli vapaasti nähtävillä yrittäjien keskustelupalstalla ja Suomen Yrittäjät ry:n Facebook -sivustolla. Sähköpostin välityksellä lähetetty linkki oli julkinen, joten vastaajat eivät olleet yksilöitävissä. Muistutuksia kyselyyn osallistumisesta ei voitu myöskään tästä syystä lähettää. Kysely avattiin 125 kertaa vastausta lähettämättä, näin ollen voidaan sanoa että kaikista kyselyn avanneista 34 % vastasi siihen. Kysymyksiin vastaaminen oli vapaaehtoista, vastauksia saatiin kuitenkin kattavasti.

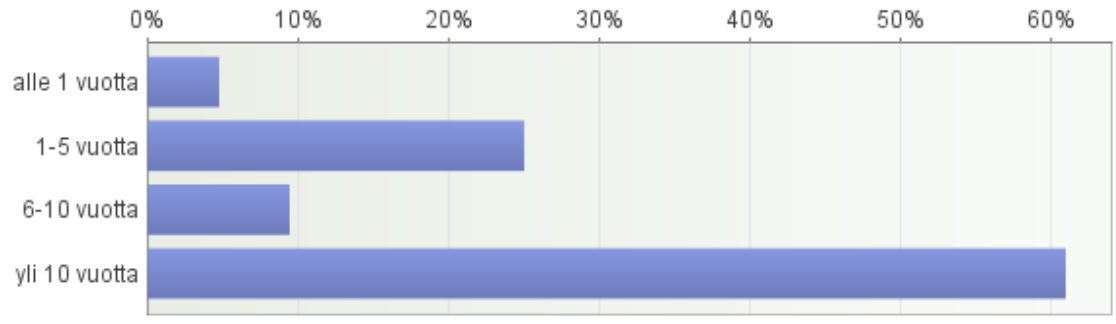
6.1 Perustiedot

Kyselyyn vastasi yhteensä 65 pk-yrityksen edustajaa, jotka jakautuivat kuvion 1 mukaisesti. Vastanneista yrityksistä 65 % oli mikroyrityksiä, 32 % pienyrityksiä ja 3 % keskisuuria yrityksiä.



Kuvio 1. Yrityksen koko

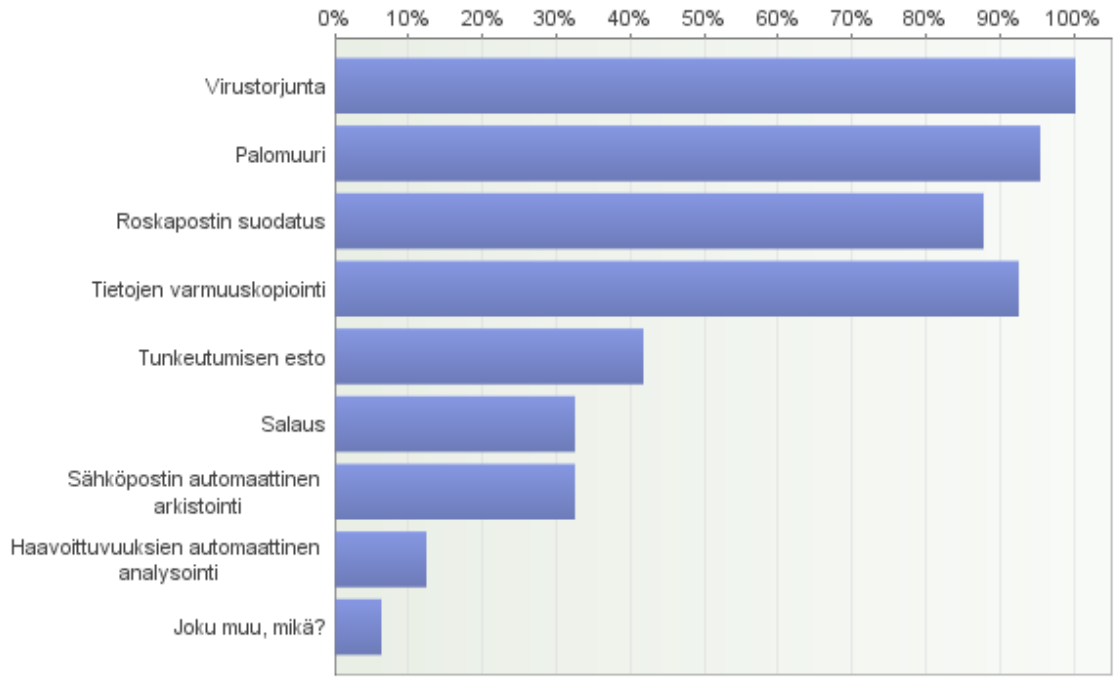
Seuraavaksi kysyttiin kuinka monta vuotta yritys on ollut toiminnassa (kuvio 2). Kyselyyn vastanneista yrityksistä 5 % oli toiminut alle vuoden, 25 % oli toiminut 25 vuotta ja 61 % oli ollut toiminnassa yli 10 vuotta.



Kuvio 2. Kuinka monta vuotta yritys on ollut toiminnassa

6.2 Tekninen tietoturva

Ensimmäinen varsinainen kysymys koski yrityksen käytössä olevia tietoturvaratkaisuja.



Kuvio 3. Yrityksen käytössä olevat tietoturvaratkaisut

Vastauksista (kuvio 3) kävi ilmi, että kaikilla tutkimukseen vastanneilla yrityksillä on käytössään virustorjuntaohjelmisto. Lähes kaikki yritykset ovat suojanneet tietoliikenteensä palomuurilla (95 %) ja suuri osa (92 %) yrityksistä varmuuskopioi tietojaan. Roskapostin suodatus on käytössä 88 %:lla vastaajista. Tunkeutumisen esto on käytössä 42 %:lla, salaus sekä sähköpostin automaattinen arkistointi 32 %:lla. Harvalla (12 %) on käytössä haavoittuvuuksien automaattinen analysointi. Joku muu tietoturvaratkaisu oli käytössä 6 % prosentilla vastaajista.

Seuraavaksi kysyttiin yrityksen teknisten tietoturva-asioiden hoidosta. Taulukosta 1 käy ilmi että yrityksen internet-yhteydet on suojattu palomuurilla melkein kaikissa yrityksissä (94 %) ja melkein kaikissa yrityksissä (95%) on tietokoneissa automaattisesti päivittyvät virustorjuntaohjelmat. Kannettavat tietokoneet on varustettu laitekohtaisella palomuurilla 65 %:ssa yrityksistä. Myös käyttöjärjestelmien päivitykset hoidetaan keskimäärin hyvin, sillä 89% yrityksistä ilmoitti että tietokoneiden käyttöjärjestelmät päivitetään säännöllisesti. Yrityksen tietokoneet on suojattu säännöllisesti vaihdettavin salasanoin noin puolella (53 %) yrityksistä, 45% ei suojaa tietokoneitaan säännöllisesti vaihdettavin salasanoin ja 2 % ei osannut vastata kysymykseen.

Taulukko 1. Miten yrityksessänne on hoidettu seuraavat tekniset tietoturva-asiat?

	Kyllä	Ei	En osaa sanoa
Yrityksen internet-yhteydet on suojattu palomuurilla.	94%	3%	3%
Tietokoneissa on automaattisesti päivittyvät virustorjuntaohjelmat.	95%	3%	2%
Kannettavat tietokoneet on varustettu laitekohtaisella palomuurilla.	65%	19%	16%
Tietokoneiden käyttöjärjestelmät päivitetään säännöllisesti.	89%	5%	6%
Yrityksen tietokoneet on suojattu säännöllisesti vaihdettavin salasanoin.	53%	45%	2%
Tallennetut tiedot varmuuskopioidaan säännöllisesti.	94%	6%	0%
Yrityksenne tärkeitä tietojärjestelmiä varten on olemassa varajärjestelmä.	57%	37%	6%
Tekniseen tietoturvaan liittyvät palvelut ostetaan ulkopuoliselta palveluntarjoajalta.	64%	34%	2%
Yhteensä	**77%**	**19%**	**4%**

94% yrityksistä tallennetut tiedot varmuuskopioidaan säännöllisesti. Yrityksen tärkeistä tietojärjestelmistä kysyttäessä 57 % ilmoitti, että tärkeitä tietojärjestelmiä varten on olemassa varajärjestelmä. Reilu kolmannes (37 %) vastaajista ilmoitti, ettei varajärjestelmää ole ja 6 % ei osannut sanoa miten asia on yrityksessä hoidettu. 64 % yrityksistä ilmoitti ostavansa tietoturvaan liittyvät palvelut ulkopuoliselta palveluntarjoajalta.

6.3 Hallinnollinen tietoturva

Seuraavassa kysymyksessä kysyttiin henkilöstöön liittyvistä tietoturva-asioista (taulukko 2). Vain neljännekselle (25 %) yrityksistä oli laadittu tietoturvapolitiikka ja viidennekselle (19 %) oli kirjallinen tietoturvasuunnitelma. Tässä on selkeästi parantamisen varaa, sillä pientäkin yritystä auttaisi jos tietoturvasta sovitut asiat olisi kirjoitettu paperille. 77 %:ssa yrityksistä on varmistettu, että henkilöstö ymmärtää oman tietoturvavastuunsa ja 60 %:ssa yrityksistä oli nimitetty tietoturvasta vastaava henkilö.

Taulukko 2. Miten yrityksessä on hoidettu nämä henkilöstöön liittyvät tietoturva-asiat?

	Kyllä	Ei	En osaa sanoa
Yritykselle on laadittu tietoturvapolitiikka.	25%	75%	0%
Yrityksellä on kirjallinen tietoturvasuunnitelma.	19%	81%	0%
Yrityksessä on varmistettu, että henkilöstö ymmärtää oman tietoturvavastuunsa.	77%	20%	3%
Yrityksessä on nimetty tietoturvasta vastaava henkilö.	60%	37%	3%
Henkilökunta on perehdytetty tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot.	74%	23%	3%
Henkilökunta on perehdytetty tunnistamaan tietojärjestelmiin liittyviä riskejä.	77%	20%	3%
Yrityksen henkilökunta on tietoinen milloin voidaan antaa ulkopuolisille yritystoiminnan kannalta luottamuksellisia tietoja.	88%	9%	3%

Henkilökunta on perehdytetty tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot 74 %:ssa yrityksistä ja henkilökunta on perehdytetty tunnistamaan tietojärjestelmiin liittyviä riskejä 77 % :ssa yrityksistä. Yrityksen henkilökunta on tietoinen milloin voidaan antaa ulkopuolisille yritystoiminnan kannalta luottamuksellisia tietoja 88 %:ssa yrityksistä. Henkilökuntaan liittyvät riskit on hoidettu suurimmassa osassa yrityksiä hyvin. Tosin 3 % vastaajista ei osannut sanoa henkilökuntaan liittyvien tietoturva-asioiden hoidosta.

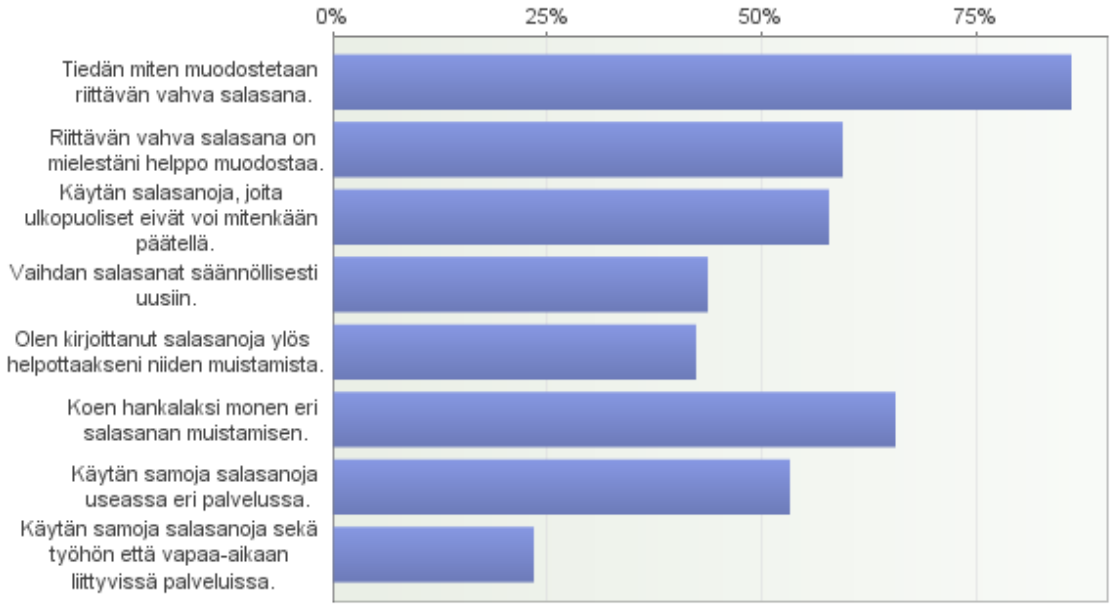
Seuraavassa kysymyksessä kysyttiin miten yrityksessä on hoidettu liiketoimintaan liittyvien riskien hoitoa ja suunnitelmallisuutta riskien varalle. Yrityksen luottamuksellisiin tietoihin liittyvät riskit oli arvioitu 65 % :ssa yrityksistä, mutta kolmannes (33 %) yrityksistä ei ollut arvioinut liiketoimintaan liittyviä riskejä. 64 %: ssa yrityksistä on ennakoitu tilanteet, jotka voivat aiheuttaa tietojen muuttumisen tai katoamisen. Kolmanneksessa (31 %) yrityksiä tällaisia tilanteita ei ollut arvioitu ja 5 % ei osannut vastata kysymykseen.

Taulukko 3. Miten yrityksessä on hoidettu liiketoimintaan liittyvät tietoturva-asiat?

	Kyllä	Ei	En osaa sanoa
Yrityksen luottamuksellisiin tietoihin liittyvät riskit on arvioitu.	65%	33%	2%
Yrityksessä on ennakoitu tilanteet, jotka voivat aiheuttaa tietojen muuttumisen tai katoamisen.	64%	31%	5%
Yrityksessä on arvioitu riskejä, jotka liittyvät tietojärjestelmien toimimattomuuteen ja siitä seuraavaan liiketoiminnan keskeytykseen.	72%	23%	5%
Yrityksessä on arvioitu mahdollisten tietojärjestelmähäiriöiden aiheuttamat menetykset.	56%	39%	5%
Yritys on tehnyt suunnitelman siltä varalta, että havaitaan tietoihin liittyviä väärinkäytöksiä?	32%	65%	3%
Yrityksellä on suunnitelma miten tilanne palautetaan normaaliksi poikkeavan tilanteen jälkeen (toipumissuunnitelma).	54%	43%	3%

Suuressa osassa (72 %) yrityksistä oli arvioitu riskejä, jotka liittyvät tietojärjestelmien toimimattomuuteen ja siitä seuraavaan liiketoiminnan keskeytykseen. 23 %:ssa yrityksistä riskejä ei ollut arvioitu ja 5 % yrityksistä ei osannut vastata kysymykseen. Mahdollisten tietojärjelmähäiriöiden aiheuttamat menetykset oli arvioitu 56 %: ssa yrityksistä, kun 39 %:ssa yrityksistä mahdollisia menetyksiä ei ollut arvioitu ja 5 % ei osannut vastata kysymykseen. Vain kolmannes (32 %) oli tehnyt suunnitelman siltä varalta, että havaitaan tietoihin liittyviä väärinkäytöksiä. Suuri osa ei siis ollut tehnyt suunnitelmaa väärinkäytösten varalle. Peräti 65 %:lta yrityksistä puuttui tällainen suunnitelma ja 3 % yrityksistä ei osannut vastata kysymykseen. Hieman yli puolet (54%) yrityksistä oli tehnyt suunnitelman, miten tilanne palautetaan normaaliksi poikkeavan tilanteen jälkeen. Tällainen toipumissuunnitelma puuttui 43 %:lta yrityksistä ja 3 % ei osannut sanoa onko suunnitelmaa tehty.

Seuraavaksi kysyttiin salasanojen käytöstä. Vastajia pyydettiin valitsemaan ne väittämät, jotka kuvaavat heidän salasanojen käyttötottumuksiaan. Kysymyksellä pyrittiin selvittämään kohdeyritysten vastuuhenkilöiden salasanojen käyttötottumuksia ja löytämään ne salasanoihin liittyvät asiat, joissa on vielä parantamisen varaa.



Kuvio 4. Salasanojen käyttötottumukset

Vastauksista (kuvio 4) käy ilmi että suuri osa (86 %) vastaajista tietää miten muodostetaan riittävän vahva salasana ja 60 % mielestä riittävän vahva salasana on helppo muodostaa. Tästä voidaan päätellä että 40 % mielestä riittävän vahvaa salasanaa ei ole helppo muodostaa. Jos tarpeeksi vahvan salasanan muodostaminen koetaan hankalana, saattaa se houkutella käyttämään liian helppoja salasanoja.

58 % vastaajista kertoi käyttävänsä salasanoja, joita ulkopuoliset eivät voi mitenkään päätellä. Vajaa puolet (44 %) vastaajista kertoi vaihtavansa salasanat säännöllisesti uusiin. Tästä voidaan päätellä että yli puolet vastaajista ei vaihda salasanojaan, ainakaan säännöllisin väliajoin. Kaksi kolmannesta (66 %) vastaajista kokeekin hankalaksi monen eri salasanan muistamisen ja noin puolet (53 %) käyttää samoja salasanoja useassa eri palvelussa. Vastaajista 23 % käyttää samoja salasanoja sekä työhön että vapaa-aikaan liittyvissä palveluissa.

Lopuksi kysyttiin avoimella kysymyksellä, mitkä ovat suurimmat puutteet yrityksen tietoturva-asioissa. Eniten mainintoja saivat seuraavat asiat:

- tiedon / osaamisen /käytettävissä olevan ajan puuttuminen / tietoturva-asioihin perehtymättömyys (eniten mainintoja)
- luottamus siihen ettei mitään tapahdu (useita mainintoja)
- liian helpot salasanat (useita mainintoja)
- salasanojen vaihtaminen uusiin liian harvoin /samat salasanat eri paikoissa (useita mainintoja)
- käyttäjät / ihmiset (useita mainintoja)
- järjestelmällinen ja säännöllinen varmuuskopiointi puuttuu /varmuuskopioinnin testaamisen puuttuminen (useita mainintoja)

Vastausten perusteella voidaan päätellä, että pk-yrityksiä huolestuttaa eniten yrityksessä olevan osaamisen, tiedon ja käytettävissä olevan ajan puute. Pk-yritykset myös luottavat liikaa siihen, ettei juuri heille tapahdu mitään. Pienemmät yritykset saattavat kokea, ettei heidän tiedoissaan ole mitään rikollisia kiinnostavaa. Tämä on kuitenkin huono tapa perustella asiaa, sillä verkkorikolliset saattavat olla kiinnostuneita myös vapaasta prosessitehosta ja levytilasta.

Liian helpot salasanat ja salasanojen vaihtaminen uusiin liian harvoin keräsi myös useita mainintoja. Myös samojen salasanojen käyttäminen useassa eri paikassa mietitytti vastaajia. Pk-yrityksissä koetaan ongelmaksi myös yleisesti lähdekirjallisuudessa mainittu tietoturvan inhimillinen puoli. Ihmisten ja järjestelmien käyttäjien koetaan olevan uhka tietoturvalle. Myös järjestelmällisen ja säännöllisen varmuuskopioinnin puuttuminen huolestuttaa pk-yritysten edustajia.

Yksittäisiä mainintoja saivat lisäksi:

- kaikki tieto/salasanat ainoastaan yhdellä henkilöllä, varahenkilön puuttuminen
- varasuunnitelman puuttuminen jos jotain tapahtuu
- häiriöiden / katoamisten aiheuttamat menetykset

- kirjallisten ohjeiden puuttuminen
- ohjelmia ei päivitetä jatkuvasti
- systemaattisuuden puute
- fyysinen tietoturva
- puutteellinen dokumentointi
- varapalvelun puuttuminen ulkoistetulle IT-tukipalvelulle
- oman IT-tukihenkilön puuttuminen
- eri aikoina hankitut koneet ja ohjelmat
- järjestelmä monimutkaistuu ja tietoturva vie laitteiston resursseja, päivitykset vaikuttavat joskus epätoivotulla tavalla toimivuuteen
- laitteiden mekaaninen kestävyys ongelmana
- asiakassuhteeseen liittyvien sähköpostien säilytys työsuhteen päättyessä
- tietoturvamenetelmien liian harva päivittäminen

Eräs vastaaja koki ongelmaksi sen, että yhden hengen yrityksessä kaikki tieto ja salasanat ovat ainoastaan yhdellä henkilöllä. Jos henkilölle tapahtuisi jotain, ei tilanteen varalle ole olemassa varasuunnitelmaa. Myös kirjallisia ohjeita ja systemaattisuutta sekä parempaa dokumentointia peräänkuulutettiin.

Eri aikoina hankitut koneet ja ohjelmat aiheuttavat myös ongelmia. Yrityksellä tulisikin olla lista kaikissa käytössä olevista laitteista ja ohjelmistoista, jotta niiden suhteen pysytään ajan tasalla. Monimutkaisen järjestelmän ja tietoturvan yhteensovittaminen koettiin joissain tilanteissa ongelmalliseksi. Tietoturvan koettiin vievän laitteiston resursseja ja päivitysten todettiin vaikuttavan joskus epätoivotulla tavalla järjestelmien toimivuuteen. Myös laitteiden mekaaninen kestävyys nähtiin ongelmana.

Eräs vastaaja koki ongelmaksi asiakassuhteisiin liittyvien sähköpostien säilytyksen työsuhteen päättyessä. Myös näitä tilanteita varten yrityksessä tulisi olla etukäteen sovitut säännöt, miten kyseisissä tilanteissa toimitaan. Asiakassuhteeseen liittyviä sähköposteja voidaan edelleen tarvita, vaikka niitä hoitanut työntekijä vaihtaisi työpaikkaa. Tässä tulee huomioida myös tietosuojaan liittyvien lakien vaatimukset.

Lopuksi vastaajien oli vielä mahdollista tarkentaa vastauksiaan tai kertoa vapaasti näkemyksiä tietoturva-asioihin liittyen. Muutama mikroyrityksen edustaja kommentoi, ettei heidän yrityksessään ei tietoturvaongelmia ole ja että tietoturva-asiat ovat pk-yrityksen kohdalla yliarvostettuja. Toisaalla vastauksissa mainittiin, että tutkittu asia on tärkeä ja erityisesti pilvipalveluiden tietoturva-asioiden käsittelylle nähtiin tarvetta. Yhden pienyrityksen edustajan mielestä tietoturvauhat ovat lisänneet yritykselle aiheutuvia kustannuksia kohtuuttoman paljon. Tässä olisikin syytä miettiä miten tietoturva-asiat saataisiin pk-yritysten kohdalla kuntoon mahdollisimman kustannustehokkaasti.

Yhdessä reilun 10 hengen yrityksestä kerrottiin että niin pienelle yritykselle ei ole mahdollista palkata omaa IT-asiantuntijaa. Riittävä asiantuntemus tietoturva- ja IT-asioihin on saavutettavissa vain ostettaessa se asiantuntijaorganisaatiolta. Tämä onkin varmasti järkevä tapa hoitaa pienen yrityksen tietoturva-asioita. Loppujen lopuksi tulee halvemmaksi ostaa palvelut asiantuntijalta, kuin käyttää omaa kallista aikaa asioihin perehtymiseen.

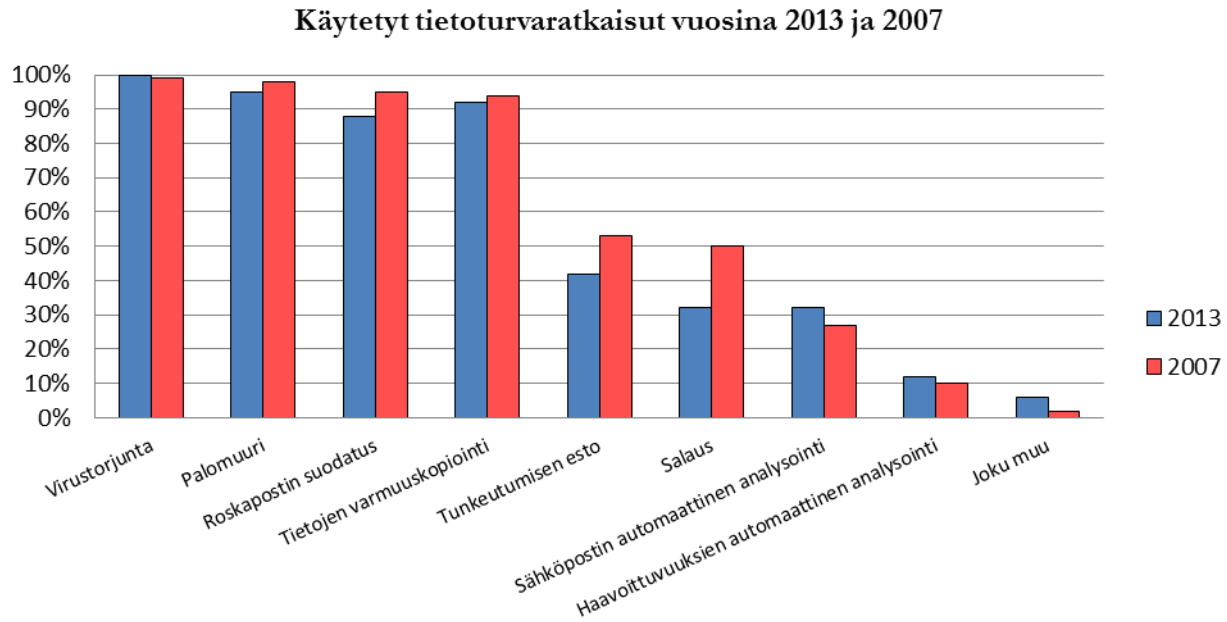
Salasanat aiheuttivat myös keskustelua. Vastaajien mielestä tunnistautumisen tulisi olla helppoa, eikä liian vaikeiden salasanojen käytössä koettu olevan mitään mieltä. Vastaajan mielestä työpaikalla on muutakin tekemistä, kuin keskittyä salasanojen muistamiseen. Salasanoja katsottiin tarvittavan liikaa ja kaivattiin järjestelyä eri tärkeysasteen salasanoille, jolloin voisi helpommin käyttää samaa salasanaa moneen eri paikkaan. Salasanojen vahvuus katsottiin tarpeelliseksi vain tärkeissä asioissa. Henkilöstölle tulisikin korostaa sitä, miksi salasanavaatimukset ovat sellaisia kuin ovat. Henkilöstön asenteet asiaa kohtaan voisivat muuttua kun he ymmärtäisivät perimmäiset syyt monimutkaisten salasanojen käyttöön.

6.4 Vertailu aiempiin tutkimuksiin

Tästä tutkimuksesta ei voi tehdä kovin yleispäteviä johtopäätöksiä pienen otoskoon (65 vastausta) perusteella, mutta jotain vertailua aikaisempiin tutkimuksiin voidaan silti suorittaa.

Tietotekniikanliitto ry:n vuoden 2007 tutkimukseen vastanneista yrityksistä lähes kaikki käytti virustorjuntaa (99 %), palomuuria (98 %), roskapostin suodatusta (95%) sekä tietojen varmuuskopiointia (94 %). Lisäksi puolet vastaajista ilmoitti käyttävänsä tunkeutumisen estoa (53 %) tai salausta (50 %). Sähköpostin automaattista arkistointia käytti 27 % vastaajista ja haavoittuvuuksien automaattinen analysointi oli käytössä 10 %:lla vastaajista. (Tietotekniikanliitto ry 2007.)

Vertailtaessa vuoden 2007 vastauksia tämän tutkimuksen tuloksiin (kuvio 5), voidaan todeta ettei tutkimustuloksissa ole merkittäviä eroja. Ainoastaan tunkeutumisen eston ja salauksen käyttö näyttäisi vähentyneen, muiden tietoturvaratkaisujen käytössä on havaittavissa pientä nousua



Kuvio 5. Käytetyt tietoturvaratkaisut vuosina 2007 ja 2013

Kauppa ja teollisuusministeriön vuonna 2006 teettämässä tutkimuksessa parhaiten kysytyistä tekniseen tietoturvaan liittyvistä asioista oli pk-yrityksissä hoidettu verkkoyhteyksien suojaaminen palomuurilla (95 %), sekä automaattisesti päivittyvällä virustorjunnalla (94 %). Sen sijaan heikoiten oli hoidettu tietokoneiden suojaaminen säännöllisesti vaihdettavilla salasanoilla (49 %) sekä tärkeimpien tietojärjestelmien vararatkaisujen järjestäminen (47 %). 84 % pk-yrityksistä ilmoitti, että tietokoneiden käyttöjärjestelmät

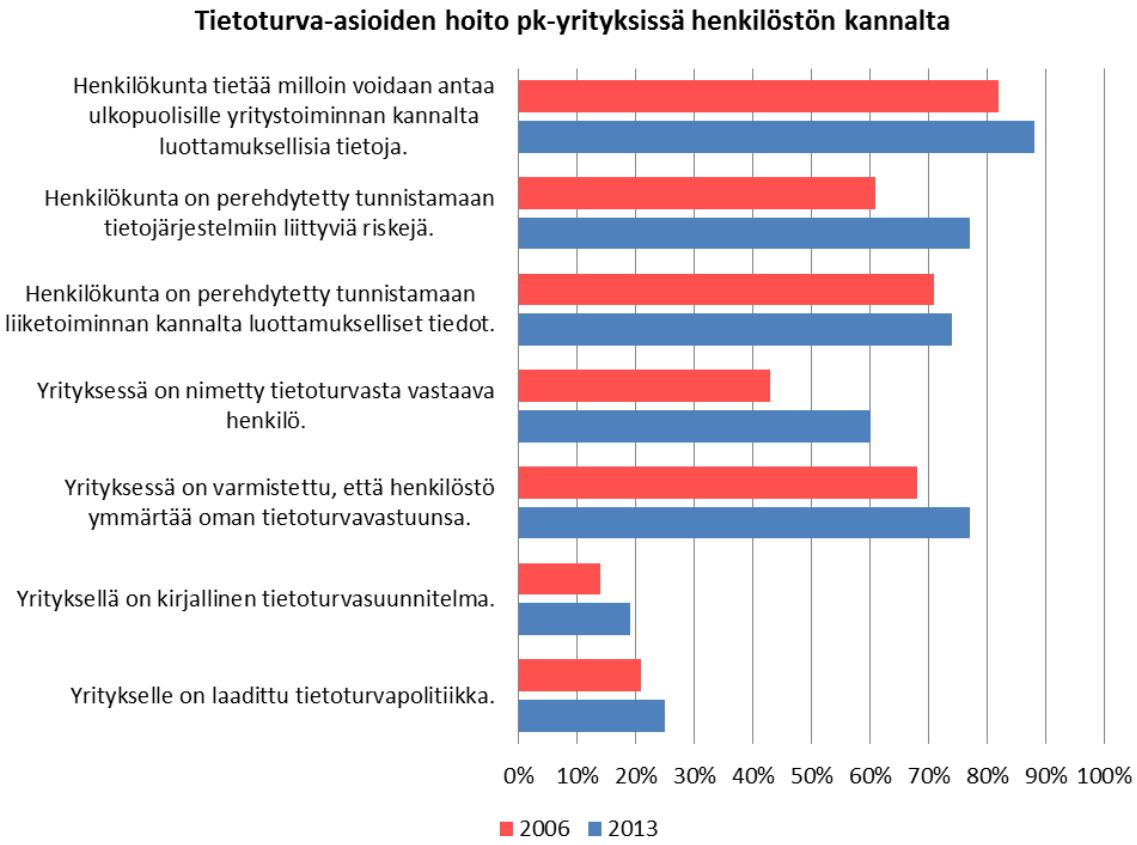
päivitetään säännöllisesti ja 68% yrityksistä ilmoitti että tietokoneille tallennetuista tiedoista otetaan varmuuskopiot säännöllisesti. (Kauppa- ja teollisuusministeriö 2007.)

Verrattaessa tämän tutkimuksen tuloksia vuoden 2006 tuloksiin (kuvio 6) voidaan havaita että kaikkien kysymysten osalta on tapahtunut jonkin verran nousua. Erityistä nousua voidaan havaita tallennettujen tietojen varmuuskopioinnissa, joka on tässä tutkimuksessa peräti 94 % kun se vuoden 2006 tutkimuksessa oli 68 %.

Kuvio 6. Teknisten tietoturva-asioiden hoito vuosina 2006 ja 2013

Vuoden 2006 tutkimuksessa eniten kehittämisen varaa löytyi hallinnollisesta tietoturvasta. Ainoastaan 14 %:lla yrityksistä oli kirjallinen tietoturvasuunnitelma ja vain 21 % yrityksistä oli laatinut tietoturvapolitiikan. Vain 43 % yrityksistä oli nimetty ja henkilöstölle tiedotettu tietoturva-asioiden vastuuhenkilö. Kyselyyn vastanneista yrityksistä 68 % ilmoitti että niissä oli varmistettu että työntekijät ymmärtävät oman tietoturvavastuunsa ja 61% ilmoitti, että yrityksen henkilökunta oli perehdytetty tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot. 82 % yrityksistä uskoi että yrityksen henkilöstö tietää miten ja milloin he voivat antaa ulkopuolisille yritystoiminnan kannalta luottamuksellisia tietoja. (Kauppa- ja teollisuusministeriö 2007.)

Verrattaessa tämän tutkimuksen tuloksia vuoden 2006 tuloksiin (kuvio 7), voidaan huomata että tulokset eivät ole merkittävästi muuttuneet. Eniten eroa vastausten välillä oli tietoturvasta vastaavan henkilön nimittämisessä. Vuoden 2006 tutkimuksessa 43 %:lla oli nimetty tietoturvasta vastaava henkilö ja tässä tutkimuksessa se oli jo 60%:lla vastaajista.



Kuvio 7. Tietoturva-asioiden hoito henkilöstön kannalta vuosina 2006 ja 2013

Vuoden 2006 tutkimuksen mukaan yritykset ovat varautuneet huonosti tietoturvariskeihin. Vain puolessa (53 %) yrityksistä oli arvioitu luottamuksellisiin tietoihin liittyvät riskit ja vain joka toinen yritys (51 %) oli arvioinut menetykset, jotka seuraavat tietojärjestelmien toimimattomuudesta. Kaikkein huonoiten yritykset olivat varautuneet mahdollisiin väärinkäytöstilanteisiin. Vain joka kolmannella (31 %) yrityksistä oli suunnitelma tilanteisin, joissa havaitaan tietoihin liittyviä väärinkäytöksiä ja vain joka toisella yrityksellä oli suunnitelma miten palauttaa tilanne normaaliksi häiriötilanteen jälkeen. (Kauppa- ja teollisuusministeriö 2007.)

Verrattaessa tämän tutkimuksen tuloksia vuoden 2006 tuloksiin (kuvio 8), voidaan huomata että tulokset eivät ole tässäkään kysymyksessä merkittävästi muuttuneet. Eniten tulokset eroavat yrityksen luottamuksellisiin tietoihin liittyvien riskien arvioinnissa ja tietojärjestelmän toimimattomuuteen ja siitä seuraavien liiketoiminnan riskien arvioinnissa.

Kuvio 8. Tietoturva-asioiden hoito liiketoiminnan kannalta vuosina 2006 ja 2013

7 Johtopäätökset ja suositukset

Pk-yrityksen tietoturva on edelleen ajankohtainen aihe, joka herättää mielipiteitä ja kiinnostusta puolesta ja vastaan. Aihe on ehdottomasti tutkimisen arvoinen nyt ja jatkossa.

7.1 Johtopäätökset

Tämän tutkimuksen tulokset ovat suuntaa antavia, mutta jotain johtopäätöksiä niistä voidaan kuitenkin tehdä. Vastauksien oikeellisuutta ei ole syytä epäillä, koska kysely tehtiin täysin anonyymisti eikä vastaajilla ollut syytä poiketa totuudesta. Tutkimustulosten luotettavuutta voidaan tarkastella vastaajien määrän perusteella ja tämän kokoisella otannalla (65) ei vielä voida tehdä kovin yleispäteviä johtopäätöksiä. Eri kokoisten yritysten vastausten vertailu ei myöskään osoittautunut mielekkääksi vastaajamäärän pienen koon vuoksi. Jos tutkimus olisi mahdollista toteuttaa suuremmalla määrällä yrityksiä, saataisiin luotettavampaa ja paremmin yleistettävissä olevaa tietoja. Suuremmalla aineistolla eri kokoisten yritysten vertailu olisi myös mielekkäämpää.

Tehdyn kyselytutkimuksen perusteella tekniset asiat on hoidettu pk-yrityksissä pääosin hyvin. Virustorjunnan ja palomuurin käyttö sekä tietojen varmuuskopiointi on suuressa osassa yrityksiä hoidettu asianmukaisesti. Näistä asioista on julkisuudessakin puhuttu paljon ja ne tuntuvat toteutuvan myös käytännön tasolla pk-yrityksissä. Itseäni ilahdutti erityisesti varmuuskopioinnin tila yrityksissä. Olin omien kokemuksieni perusteella arvellut, että varmuuskopioinnin hoitamisessa olisi vielä toivomisen varaa.

Kuten aiemmin tehdyissä tutkimuksissa on todettu, myös tästä tutkimuksesta voidaan tehdä johtopäätös että yritysten hallinnollisessa tietoturvassa on edelleen eniten parantamisen varaa. Tietoturvapolitiikan ja kirjallisen tietoturvasuunnitelman puuttumisen voi toki ymmärtää pienemmissä yrityksissä, mutta silti tärkeimpien tietoturvaperiaatteiden kirjaaminen ylös voisi edistää pienenkin yrityksen tietoturva-asioita merkittävästi. Liiketoimintaan liittyvät tietoturva-asiat oli tutkimuksen mukaan hoidettu kohtalaisen hyvin. Luottamuksellisiin tietoihin kohdistuvia riskejä kannattaisi kuitenkin arvioida kattavammin, jotta voitaisiin varautua mahdollisiin ongelmatilanteisiin. Myös pk-

yrityksellä olisi hyvä olla suunnitelma sen varalle, että havaitaan väärinkäytöksiä tai tietojärjestelmähäiriöiden aiheuttamia menetyksiä. Oli kuitenkin ilahduttava huomata että suuressa osassa yrityksistä oli arvioitu riskejä, jotka liittyvät tietojärjestelmien toimimattomuuteen ja siitä seuraavaan liiketoiminnan keskeytykseen.

Salasanoista on ollut julkisudessa paljon puhetta, valitettavasti lähinnä silloin kun salasanoja on joutunut vääriin käsiin. Myös tämän tutkimuksen mukaan salasanojen käytössä on edelleen parantamisen varaa. Suurin osa yritysten edustajista tietää miten muodostetaan riittävän vahva salasana, mutta tästä huolimatta yrityksissä käytetään liian helppoja ja turvattomia salasanoja. Salasanoja myös kirjoitetaan vastoin ohjeita ylös niiden muistamiseksi, ja lisäksi eri järjestelmässä saatetaan käyttää samoja salasanoja. On toki inhimillistä, ettei henkilö voi ulkoa muistaa useita eri salasanoja useisiin eri järjestelmiin. Tämän asian parantamiseksi yritysten tulisi rakentaa järjestelmänsä niin, että erilaisia salasanoja tarvitaan mahdollisimman vähän. Onneksi suurin osa yritysten edustajista on kuitenkin sisäistänyt sen, että työhön ja vapaa-aikaan liittyvissä palveluissa ei tule käyttää samoja salasanoja.

7.2 Tutkimuksen hyödynnettävyys ja suositukset

Tämän tutkimuksen tuloksia voidaan hyödyntää suunniteltaessa pk-yrityksille kohdistettuja tiedotuskampanjoita tietoturvasta. Tämän tutkimuksen pohjalta etenkin tietoturvan suunnitelmalliseen toteuttamiseen ja salasanoihin liittyvät asiat kaipaavat vielä ohjeistusta ja muistutusta. Näen pk-yritysten tietoturva-asioissa vielä paljon parantamisen varaa ja tietoturva-asenteiden muuttamiseksi on edessä vielä paljon töitä. Tietoturvaa ei tulisi nähdä välttämättömänä pahana, joka vie aikaa ja aiheuttaa kustannuksia. Hyvin hoidettu tietoturva on yritykselle kunnia-asia ja se voi olla myös yrityksen kilpailuvaltti markkinoilla.

Suosittelen tämän tutkimuksen perusteella pk-yrityksiin kohdistettua tietoturva-asioista tiedottamista. Internetissä on olemassa joitain yrityksille suunnattuja oppaita. En osaa sanoa miten tunnettuja ohjesivustot ovat pk-yritysten keskuudessa ja miten paljon niitä hyödynnetään. Eniten ohjeistusta kaipaavat varmasti ne yritykset, jotka eivät ohjeita

ymmärrä itse etsiä. Tulevaisuudessa tietoturvaohjeistus voitaisiin integroida muun ohjeistuksen yhteyteen esimerkiksi aloittaville yrittäjille.

Pk-yritykset ovat ilmaisseet huolensa pilvipalveluiden tietoturvasta ja myös muutama tämän työn kyselytutkimuksen vastannut mainitsi asiasta avoimissa kysymyksissä. Tämän työn puitteissa pilvipalveluiden tietoturvaa ei ollut mahdollista tutkia ja ehdotankin että asiaa tutkittaisiin puolueettomasti ja tutkimustuloksista tiedotettaisiin pk-yritysten edustajille.

Kuten ennakkoon odotin, tietoturva-asiat koetaan pienissä yrityksissä tärkeiksi, mutta käytännön osaamista on liian vähän. Pienessä yrityksissä tietoturva-asiat voivat jäädä sen työntekijän hoidettavaksi, joka niistä sattuu eniten tietämään. Erillistä tietoturvasta vastaavaa henkilöä ei välttämättä voida pienessä yrityksessä palkata, eikä ulkopuolista konsultointiapua välttämättä koeta tarpeelliseksi ennen kuin ongelma on jo olemassa.

Varmuuskopionti oli hoidettu paremmin kuin olisin omien kokemuksien perusteella arvioinut. Toki pitää muistaa, ettei varmuuskopiointi ei vieläkään ole kaikilla yrityksillä käytössä. Jos tietokone tällaisessa tilanteessa yllättäen rikkoutuu, niin pahimmassa tapauksessa ainoastaan paperille tulostetut dokumentit säilyivät. Tällainen tapahtuma voi aiheuttaa todella paljon harmia, ylimääräistä työtä ja kustannuksia, vaikka tiedon varmistus olisi ollut hoidettavissa suhteellisen pienellä vaivalla. Yleistyvät pilvipalvelut voivat osaltaan ratkaista tätä ongelmaa kun varmuuskopiointi hoituu automaattisesti.

Pilvipalveluita hyödynnettäessä palvelut ovat käytettävissä laitteesta ja paikasta riippumatta missä vain. Ohjelmistojen päivitykset ja varmuuskopiointi on ulkoistettu pilvipalvelun ylläpitäjälle. Tällaiset palvelut saattavat myös vaatia vahvempaa salasanaa ja salasanan vaihtoon voidaan pakottaa säännöllisin väliajoin. Pienelle yritykselle pilvipalvelut voisivat olla mahdollisuus hoitaa ainakin varmuuskopiointi ja ohjelmistojen päivitykset automaattisesti. Yrityksen tulee kuitenkin myös arvioida pilvipalveluiden käyttöönotosta aiheutuvat tietoturvauhkat palveluita harkitessaan.

Useissa lähteissä mainittiin keskeisenä tietoturvaongelmana henkilöstön käyttäytyminen ja ihmisiä pidetään yleisesti tietoturvan heikoimpana lenkkinä. Yritykset kokevat kyllä

löytävänsä tietoa, jos sitä etsivät, mutta konkreettisille ohjeille tuntuu silti olevan kysyntää. Pk-yrityksessä kaikki käytettävissä oleva aika saattaa mennä yrityksen ydintoimintojen ylläpitämiseen eikä tietoturva-asioille välttämättä jää juuri aikaa. Aihe koetaan kyllä tärkeäksi, mutta käytännössä tietoturvasta vastaa usein virustorjuntaohjelma ja palomuuri. Käyttöjärjestelmiä ja ohjelmistoja päivitetään vaihtelevasti.

Henkilöstön käyttäytymiseen liittyy läheisesti myös salasanat ja käytettyjen salasanojen heikkous. Vaikka hyvien salasanojen tärkeydestä muistutetaan jatkuvasti, nämä asiat eivät tunnu toteutuvan käytännössä. Useimmat kyllä tietävät, millainen hyvä salasana on, mutta salasanaksi saatetaan silti valita helposti arvattavissa oleva heikko salasana. Salasanan vaihtaminen säännöllisin väliajoin koetaan myös hankalaksi ja sen koetaan vaikeuttavan työtä.

Normaalisti yrityksen työntekijällä on muistettavanaan salasanoja moneen eri palveluun. Jos työntekijä käyttää työsähköpostiosoitetta ja samoja salasanoja kirjautuessaan vapaa-ajallaan nettipalveluihin, voi tämä muodostua merkittäväksi turvallisuusriskiksi. Tietoturvaohjeistuksissa korostetaan, että jokaiseen palveluun tulisi olla vahva tietoturvallinen salasana ja samaa salasanaa ei saisi käyttää eri paikoissa. Monien eri salasanojen muistaminen koetaan kuitenkin hankalaksi ja se myös lisää kiusausta kirjoittaa salasanat ylös.

Salasana ei myöskään saa olla helposti arvattavissa henkilötietojen perusteella, mutta silti monella on käytössä salasanana esimerkiksi etu- tai lempinimi ja syntymävuosi. Käytännön elämässä näitä huonoina pidettyjä salasanoja käytetään kaikesta huolimatta yleisesti jopa arkaluontoisenkin tiedon suojaamiseen. Salasanan vaihtaminen koetaan negatiivisena asiana ja myös uusien salasanojen keksimistä pidetään haastavana. Tietovuotojen myötä järjestelmien käyttäjätunnuksia ja salasanoja on vuotanut internetiin.

7.3 Oppimisprosessi

Opin opinnäytetyöprosessin aikana paljon uutta. Aihealueen teoria oli osittain verran tuttua aikaisempien opintojen ja oman kiinnostuksen perusteella hankitun osaamisen

kautta, mutta matkan varrella tarttui mukaan myös paljon uutta tietoa ja osaamista. Vaikka tietoturva oli aihealueena jonkin verran tuttu jo ennestään, antoi lähdekirjallisuuteen perehtyminen laaja-alaisen kuvan tietoturvallisuuden kentästä. Opin myös sen että tietoturva aihealueena on äärettömän laaja ja monta kertaa tuli vastaan asia, jota olisin halunnut tarkastella tarkemmin, mutta se ei ollut tämän opinnäytetyön puitteissa mahdollista. Tämän opinnäytetyön avulla hankitusta laaja-alaisesta tietoturvaosaamisesta tulee varmasti olemaan hyötyä myös tulevaisuudessa.

Opinnäytetyöprosessi venyi alkuperäistä suunnitelmaa pitemmäksi erinäisistä syistä johtuen. Lisäksi muista töistä ja velvollisuuksista johtuen välillä hyvinkin kiireinen aikataulu aiheutti omat haasteensa. Haasteista kuitenkin selvittiin ja koen oppineeni paljon opinäytetyöprosessin aikana itsenäisestä työskentelystä ja itsenäisen projektin läpiviennistä. Opin itsestäni myös sen, että paineen alla työskentely tuntuu sopivan minulle, vaikka se välillä hieman stressaavaa olikin. Opin paljon myös suunnittelun tärkeydestä. Erityisesti ajankäytön suunnittelu osoittautui tärkeäksi kiireisessä prosessissa. Sain myös kokea että kun työskentelyyn ryhtyy silloin kun on suunnitellut, on työn tekeminen paljon helpompaa ja aikaansaannokset innostavat jatkamaan.

Pk-yrityksen tietoturva on hyvin laaja aihekokonaisuus ja tässä työssä oli mahdollista käsitellä aihetta vain pintaraapaisun verran. Suomenkielistä laadukasta kirjallisuutta aiheesta on saatavilla runsaasti ja myös internetissä on paljon ohjeita aiheeseen liittyen. Erityisesti Valtiovarainministeriön kehittämä ja ylläpitämä VAHTI -ohjeistus on mainitsemisen arvoinen. Valtiohallinnon tietoturvallisuuden johtoryhmän työn tuloksena on aikaansaatu yksi maailman kattavimmista yleisistä tietoturva-ohjeista. VAHTI -tietoturvaohjeet on kehitetty julkis- ja valtionhallinnon tarpeisiin, mutta kattavia ohjeita voidaan soveltaa myös pienempien yritysten tarpeisiin.

8 Lähteet

Andreasson, A., Koivisto, J., Ylipartanen, A. 2013a. Tietosuojavastaavan käsikirja. Tietosanoma Oy. Helsinki.

Andreasson, A. & Koivisto, J. 2013b. Tietoturvaa toteuttamassa. Tietosanoma Oy. Helsinki.

Hakala, Vainio, Vuorinen 2006. Tietoturvallisuuden käsikirja. Dodenco Finland Oy. Jyväskylä.

Heljaste, Korkiamäki, Laukkala, Mustonen, Peltonen, Vesterinen 2008. Yrityksen turvallisuusopas. Helsingin seudun kauppakamari.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2010. Tutki ja kirjoita. 15.-16. painos. Tammi. Helsinki.

Kauppa- ja teollisuusministeriö 2007. PK-yritysten tietoturvakysely 2006. Luettu 18.5.2013. Luettavissa: http://www.ek.fi/ek/fi/yrittajyys_ym/yrittajyys/tietoa_pk-yrityksista/liitteet/Pk-yritystentietoturvakysely.pdf

Keskuskauppakamari ja Helsingin seudun kamari 2012. Yritysten rikosturvallisuus 2012: Riskit ja niiden hallinta. Luettu 26.5.2013. Luettavissa: http://kauppakamari.fi/wp-content/uploads/2012/01/Yritysten_rikosturvallisuus_2012-.pdf

Laaksonen, Nevasalo, Tomula 2006. Yrityksen tietoturvakäsikirja. Edita Publishing Oy.

Lacey D., James B. 2010: Review of Availability of Advice on Security for Small/Medium Sized Organisations. Luettavissa: http://www.ico.org.uk/upload/documents/library/corporate/research_and_reports/review_availability_of_%20security_advice_for_sme.pdf. Luettu 27.6.2013

Puhakainen, P. 2006. A design theory for information security awareness. Väitöskirja. Oulun Yliopisto. Luettavissa: http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf. Luettu 27.4.2013.

Salo, I. 2010. Cloud Computing palvelut verkossa. WSOYpro Oy. Jyväskylä

Salminen, M. 2009. Tietosuoja sähköisessä liiketoiminnassa. Talentum Media Oy.

Tietotekniikan liitto ry, 2007. Pk-tietoturvatutkimus. Luettavissa: http://www.ttlry.fi/sites/ttl.ttlry.mearra.com/files/file-uploads/Tutkimus/PK-tietoturvatutkimus/pk-yritysten%20tietoturvakysely%202007.5.21_SZ.pdf. Luettu: 16.5.2013.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf. Luettu 27.4.2013.

Valtiovarainministeriö 2008a. Tietoturvallisuus on asenne! Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Tietot/vahti6_taitto_NETTI_%2b_KANNET.pdf. Luettu 2.6.2013.

Valtiovarainministeriö 2008b. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf. Luettu 2.6.2013.

Valtiovarainministeriö 2012. Teknisen ICT-ympäristön tietoturvataso-ohje. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20121122Teknis/ICT_taitto.pdf.

9 Liitteet

Liite 1. Tietoturvakysely pk-yrityksille

1. Yrityksen koko
- Mikroyritys (1-9 henkilöä)
- Pienyritys (10-49 henkilöä)
- Keskisuuri yritys (50-249 henkilöä)

2. Kuinka monta vuotta yritys on toiminut?
- Alle 1 vuotta
- 1-5 vuotta
- 6-10 vuotta
- yli 10 vuotta

3. Yrityksen liikevaihto viimeksi päättyneellä tilikaudella (€)

4. Mitä seuraavista tietoturvaratkaisuista yrityksellä on käytössä?
- Virustorjunta
- Palomuuri
- Roskapostin suodatus
- Tietojen varmuuskopiointi
- Tunkeutumisen esto
- Salaus
- Sähköpostin automaattinen arkistointi
- Haavoittuvuuksien automaattinen analysointi
- Joku muu, mikä?

5. Miten yrityksessänne on hoidettu seuraavat tekniset tietoturva-asiat?

- Yrityksen internet-yhteydet on suojattu palomuurilla.
- Tietokoneissa on automaattisesti päivittyvät virustorjuntaohjelmat.
- Kannattevat tietokoneet on varustettu laitekohtaisella palomuurilla.
- Tietokoneiden käyttöjärjestelmät päivitetään säännöllisesti.
- Yrityksen tietokoneet on suojattu säännöllisesti vaihdettavin salasanoin.
- Tallennetut tiedot varmuuskopioidaan säännöllisesti.
- Yrityksenne tärkeitä tietojärjestelmiä varten on olemassa varajärjestelmä.
- Tekniseen tietoturvaan liittyvät palvelut ostetaan ulkopuoliselta palveluntarjoajalta.

6. Miten yrityksessänne on hoidettu seuraavat henkilöstöön liittyvät asiat?

- Yritykselle on laadittu tietoturvapolitiikka
- Yrityksessä on varmistettu, että henkilöstö ymmärtää oman tietoturvavastuunsa.
- Yrityksessä on nimetty tietoturvasta vastaava henkilö.
- Henkilökunta on perehdytetty tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot.
- Henkilökunta on perehdytetty tunnistamaan tietojärjestelmiin liittyviä riskejä.
- Yrityksen henkilökunta on tietoinen milloin voidaan antaa ulkopuolisille yritystoiminnan kannalta luottamuksellisia tietoja.

7. Miten yrityksessänne on hoidettu seuraavat liiketoimintaan liittyvät tietoturva-asiat?

- Yrityksen luottamuksellisiin tietoihin liittyvät riskit on arvioitu.
- Yrityksessä on ennakoitu tilanteet, jotka voivat aiheuttaa tietojen muuttumisen tai katoamisen.
- Yrityksessä on arvioitu riskejä, jotka liittyvät tietojärjestelmien toimimattomuuteen ja siitä seuraavaan liiketoiminnan keskeytykseen.
- Yrityksessä on arvioitu mahdollisten tietojärjestelmähäiriöiden aiheuttamat menetykset
- Yritys on tehnyt suunnitelman siltä varalta, että havaitaan tietoihin liittyviä väärinkäytöksiä.

– Yrityksellä on suunnitelma miten tilanne palautetaan normaaliksi poikkeavan tilanteen jälkeen (toipumissuunnitelma).

8. Valitse väittämät, jotka kuvaavat salasanojen käyttöäsi.

– Tiedän miten muodostetaan riittävän vahva salasana
– Riittävän vahva salasana on mielestäni helppo muodostaa.
– Käytän salasanoja, joita ulkopuoliset eivät voi mitenkään päätellä
– Vaihdan salasanat säännöllisesti uusiin
– Olen kirjoittanut salasanoja yylös helpottaakseni niiden muistamista.
– Koen hankalaksi monen eri salasanan muistamisen.
– Käytän samoja salasanoja useassa eri palvelussa.
– Käytän samoja salasanoja sekä työhön että vapaa-aikaan liittyvissä palveluissa.

9. Mitkä ovat mielestänne suurimmat puutteet yrityksenne tietoturva-asioissa?

10. Tässä voit halutessasi tarkentaa vastauksiasi tai kertoa vapaasti näkemyksiäsi tietoturva-asioihin liittyen.